kaspersky

Kaspersky Industrial CyberSecurity for Nodes 5.0

© 2026 AO Kaspersky Lab

Contents

Kaspersky Industrial CyberSecurity for Nodes
- What's new
- Fixed issues
- Distribution kit
- Hardware and software requirements
- Supported versions of Kaspersky Security Center
- Kaspersky Virus Removal Tool
- Functional requirements and limitations
  - Installing and removing the application
  - System Integrity Monitoring
  - Firewall
  - Limitations on outdated Windows versions
  - Integration with Kaspersky Security Center
  - Other limitations
- Typical deployments
- Compatibility with other applications

Installing and removing the application
- Installation planning
  - Selecting administration tools
  - Selecting the installation type
  - Ports used
- Installing and uninstalling the application using a wizard
  - Installing using the Setup Wizard
    - Kaspersky Industrial CyberSecurity for Nodes installation
    - Kaspersky Industrial CyberSecurity for Nodes Console installation
    - Advanced settings after installation of the Application Console on another device
    - Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation
      - Starting and configuring the Update of databases and application modules task
      - Critical Areas Scan
  - Modifying the set of components and repairing Kaspersky Industrial CyberSecurity for Nodes
  - Uninstalling using the Setup Wizard
    - Kaspersky Industrial CyberSecurity for Nodes uninstallation
    - Kaspersky Industrial CyberSecurity for Nodes Console uninstallation
- Installing and uninstalling the application from the command line
  - About installing and uninstalling Kaspersky Industrial CyberSecurity for Nodes from command line
  - Kaspersky Industrial CyberSecurity for Nodes software component codes for the Windows Installer service
  - Installation and recovery settings, and Windows Installer command-line options
  - Example commands for installing Kaspersky Industrial CyberSecurity for Nodes
  - Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation
  - Adding / removing components. Sample commands
  - Kaspersky Industrial CyberSecurity for Nodes uninstallation. Sample commands
  - Return codes

Installing and uninstalling the application using Kaspersky Security Center
General information about installing via Kaspersky Security Center
Rights to install or uninstall Kaspersky Industrial CyberSecurity for Nodes
Installing Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center
Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation
Installing the Application Console via Kaspersky Security Center
Uninstalling Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center
Changing the set of application components using Kaspersky Security Center
Installing and uninstalling the application via Active Directory group policies
Installing Kaspersky Industrial CyberSecurity for Nodes via Active Directory group policies
Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation
Uninstalling Kaspersky Industrial CyberSecurity for Nodes via Active Directory group policies
Kaspersky Industrial CyberSecurity for Nodes install and uninstall logs
System changes after Kaspersky Industrial CyberSecurity for Nodes installation
Kaspersky Industrial CyberSecurity for Nodes processes
Checking Kaspersky Industrial CyberSecurity for Nodes functions. Using the EICAR test virus
About the EICAR test virus
Checking the Real-Time File Protection and On-Demand Scan features
Upgrading older versions of Kaspersky Industrial CyberSecurity for Nodes to version 5.0
Updating Kaspersky Industrial CyberSecurity for Nodes
Updating Kaspersky Industrial CyberSecurity for Nodes Administration Tools
Migrating policies and tasks
Migration of settings of the application version being updated
Correspondence of components and tasks in Kaspersky Industrial CyberSecurity for Nodes versions 4.0 and 5.0
Installing and removing Kaspersky Security Gateway
Updating Kaspersky Security Gateway
Installing Kaspersky Security Gateway using the Setup Wizard
Step 1. Verifying installation requirements
Step 2. Welcome page of the installation procedure
Step 3. Viewing the End User License Agreement and Privacy Policy
Step 4. Selecting the destination folder
Step 5. Selecting components
Step 6. Configuring the connection to the SCADA system
Step 7. Installing Kaspersky Security Gateway
Installing Kaspersky Security Gateway from the command line
Removing Kaspersky Security Gateway
Step 1. Saving Kaspersky Security Gateway data for future use
Step 2. Removing Kaspersky Security Gateway
Installing OPC Core Components Redistributables
Application interface
Working with the Administration Plug-in
Managing Kaspersky Industrial CyberSecurity for Nodes from Kaspersky Security Center
Managing application settings
Configuring general application settings in Kaspersky Security Center
Configuring interface and scan settings in Kaspersky Security Center
Configuring security settings in Kaspersky Security Center

Configuring connection settings using Kaspersky Security Center
Configuring the local task run mode
Configuring Quarantine and Backup settings in Kaspersky Security Center
Creating and configuring policies
Creating a policy
Configuring a policy
Creating and configuring tasks using Kaspersky Security Center
About task creation in Kaspersky Security Center
Creating a task using Kaspersky Security Center
Going to the local task settings and general application settings for an individual computer
Configuring group tasks in Kaspersky Security Center
Application activation task
Update task
Application Integrity Control
Scheduling tasks
Reports in Kaspersky Security Center
Real-Time Protection status
Working with the Kaspersky Industrial CyberSecurity for Nodes Console
Starting the Application Console
Kaspersky Industrial CyberSecurity for Nodes Console interface
Kaspersky Industrial CyberSecurity for Nodes Console window
System Tray Icon in the notification area
Configuring general settings via the Application Console
Managing Kaspersky Industrial CyberSecurity for Nodes tasks
Kaspersky Industrial CyberSecurity for Nodes task categories
Starting, pausing, resuming, and stopping tasks manually
Scheduling tasks
Using user accounts to start tasks
About using accounts to start tasks
Specifying a user account to start a task
Importing and exporting settings
About importing and exporting settings
Exporting settings
Importing settings
Viewing protection status and Kaspersky Industrial CyberSecurity for Nodes information
How to configure Backup settings in the Application Console
Working with the Web Plug-in from Web Console
Managing Kaspersky Industrial CyberSecurity for Nodes from Web Console
Web Plug-in limitations
Managing application settings
Configuring general application settings in Web Plug-in
Configuring interface and scan settings in Web Plug-in
Configuring security and reliability settings in Web Plug-in
Configuring connection settings in Web Plug-in
Configuring scheduled start of local tasks in Web Plug-in
Configuring Quarantine and Backup settings in Web Plug-in
Creating and configuring policies

- Creating and configuring tasks using Kaspersky Security Center
  - About task creation in Web Plug-in
  - Creating a task in Web Plug-in
  - Configuring group tasks in Web Plug-in
    - Configuring the Application activation task in Web Plug-in
    - Configuring the Update task in Web Plug-in
  - Scheduling tasks
- Reports in Kaspersky Security Center

Application licensing
- About the End User License Agreement
- About the license
- About license certificate
- About the key
- About the key file
- About activation code
- Activating the application with a key file
- Activating the application with an activation code
- Viewing information about current license
- Renewing license
- Deleting the key

Starting and stopping Kaspersky Industrial CyberSecurity for Nodes
- Starting and stopping the application
- Pausing and resuming computer protection and control

Compact Diagnostic Interface
- About the Compact Diagnostic Interface
- Reviewing the Kaspersky Industrial CyberSecurity for Nodes status via the Compact Diagnostic Interface
- Reviewing security event statistics
- Reviewing current application activity
- Configuring application tracing and memory dump recording

Kaspersky Industrial CyberSecurity for Nodes self-defense
- Enabling and disabling Self-Defense
- Supporting AM-PPL technology
- Protecting operating system services
- Configuring user permissions to manage Kaspersky Industrial CyberSecurity for Nodes
- Configuring user access permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service
- Password-protected access to Kaspersky Industrial CyberSecurity for Nodes functionality
- Secure Desktop notifications

Trusted zone
- Creating a scan exclusion
- Selecting types of detectable objects
- Editing the list of trusted applications
- Creating a local trusted zone
- Exporting and importing the trusted zone
- Using trusted system certificate storage
- Predefined scan exclusions and trusted applications
- Industrial software exclusion profiles

Real-Time File Protection
About the task protection scope and security settings
Predefined protection scopes
About predefined security levels
File extensions scanned by default by the Real-Time File Protection component
Configuring Real-Time File Protection component
Configuring the protection scope for the Real-Time File Protection component
Configuring security settings manually
Container Scan
KSN Usage
Enabling the use of Kaspersky Security Network
Kaspersky Security Network usage statistics
Limitations of Kaspersky Private Security Network
KSN Proxy settings
Exploit Prevention
Exploit Prevention mode
Enabling and disabling Exploit Prevention
Enabling and disabling memory protection
Creating the list of protected processes
Remediation Engine
Anti-Cryptor
Enabling and disabling encryption protection for local folders
Protection of shared folders against external encryption
Enabling and disabling protection of shared folders against external encryption
Editing the protection scope
Adding trusted computers for external data encryption
Configuring the blocking period of an untrusted computer
Exporting and importing a list of exclusions from protection of shared folders against external encryption
Network Threat Protection
Enabling and configuring Network Threat Protection
Creating an exclusion from blocking
Exporting and importing a list of exclusions from protection of shared folders against external encryption
AMSI Scanner
Enabling and disabling AMSI Scanner
AMSI Scanner settings
Applications Launch Control
About Applications Launch Control rules
About Software Distribution Control
About the Rule Generator for Applications Launch Control
Enabling and configuring Applications Launch Control
Configuring Software Distribution Control
Working with Applications Launch Control rules
Adding Applications Launch Control rules
Adding trigger conditions for the Applications Launch Control rule
Adding exclusions from an Applications Launch Control rule scope
Permitting all applications to run

Exporting Applications Launch Control rules
Generating a TXT file with a selection of Kaspersky Security Center blocked application events
Configuring Rule Generator for Applications Launch Control group task
Creating rules using a Rule Generator for Applications Launch Control group task.
Device Control
Device Access Rules
Managing access to devices by type
Control of Wi-Fi connections
Control of printing
Input device control (HID)
Managing access to mobile devices
Monitoring usage of removable drives
Managing access to Bluetooth devices
Differentiation of user access rights to devices
About Rule Generator for Device Control
Adding trusted devices
Exporting and importing the list of trusted devices
Firewall
About Firewall rules
Configuring the Firewall
Configuring general Firewall settings
Creating and configuring Firewall rules
Enabling and disabling Firewall rules
BadUSB Attack Prevention
System Integrity Monitoring
About System Integrity Monitoring rules
Real-Time System Integrity Monitoring
On-Demand System Integrity Check
Exporting and importing System Integrity Monitoring rules
Viewing System Integrity Monitoring reports
Log Inspection
Adding custom rules
Configuring predefined rules
Performance Analyzer
On-Demand Scan
About On-Demand Scan tasks
About the task scan scope and security settings
Predefined scan scopes
Online storage file scanning
About predefined security levels
Removable drives scan
Default On-Demand Scan tasks settings
Managing On-Demand Scan tasks
Creating an On-Demand Scan task
Running an On-Demand Scan task in the background
Registering execution of a Critical Areas Scan
Configuring the scan scope in the On-Demand Scan task

Configuring the On-Demand Scan task settings
Configuring Removable Drives Scan
Selecting predefined security levels for On-Demand Scan tasks
Configuring security settings manually
On-Demand Scan task statistics
Industrial Network Protection
About PLC Project Integrity Check
Configuring PLC Project Integrity Check task
Configuring PLC Project Investigation
Configuring PLC Project Integrity Check
Enabling and Disabling PLC Project Integrity Check
About the PLC configurations Registry
Configuring PLC Registry
Security audit
Limitations for Security Audit task settings
Supported OVAL scan types
Managing Security Audit tasks
Creating and configuring the Security Audit task with the default settings
Configuring Security Audit task settings using the Kaspersky ICS CERT vulnerabilities database for SCADA
Configuring Security Audit task settings using a security and standards compliance configuration
Configuring Security Audit task settings using a custom rule database from the Kaspersky Security Center repository
Configuring the Security Audit task settings using a custom database from file
Viewing the Security Audit task execution results
Exporting the Security Audit task execution results to a separate file
Creating a thumbprint for the certificate for signing files with OVAL or XCCDF rules
Creating a Kaspersky Security Center installation package with custom OVAL or XCCDF rules
Using Kaspersky Security Gateway
Diagnostic information
Limitations and known issues of Kaspersky Security Gateway
Kaspersky Security Gateway Console interface
Configuring a connection with Kaspersky Security Center
Configuring a connection with Kaspersky Industrial CyberSecurity for Networks
Configuring the DCOM protocol
Configuring data transfer settings using communication protocols
Configuring data transfer using IEC 60870-5-104 protocol
Configuring data transfer using OPC DA protocol
Configuring data transfer using OPC UA protocol
Configuring data transfer using a configuration file
Configuring Kaspersky Security Gateway additional settings
Viewing Kaspersky Security Gateway events
BitLocker Full Disk Encryption management
Starting BitLocker Drive Encryption
Decrypting a hard drive protected by BitLocker
Restoring access to a drive protected by BitLocker
Pausing BitLocker protection to update software

Integrating with third-party systems
Performance counters for System Monitor
Number of requests not processed due to a lack of resources
Number of requests submitted for processing
Number of objects processed per second
Number of elements in the infected objects queue
Total number of requests denied
Total number of requests skipped
Maximum number of file interception dispatcher streams
Average number of file interception dispatcher streams
Kaspersky Industrial CyberSecurity for Nodes SNMP counters and traps
Kaspersky Industrial CyberSecurity for Nodes SNMP counters
Performance counters
Backup counter
General counters
Update counter
Real-Time File Protection counters
AMSI Scanner counters
Kaspersky Industrial CyberSecurity for Nodes SNMP traps and their options
Kaspersky Industrial CyberSecurity for Nodes SNMP traps options descriptions and possible values
WMI Integration
Kaspersky Industrial CyberSecurity for Nodes database and software modules update
Updating databases and application modules
About Update tasks
Kaspersky Industrial CyberSecurity for Nodes databases and modules update schemes
Configuring Update tasks
SMU update of the application
Secure copying of application databases
Secure update of application databases
Rolling back Kaspersky Industrial CyberSecurity for Nodes database updates
Update task statistics
Detection and Response solutions
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
Solution architecture
Compatibility with Kaspersky applications
Deployment and initial setup
Solution activation
Configuring threat report for viewing alert details
Adding EDR alerts widget
Monitoring the solution performance on devices
Upgrading to Kaspersky Industrial CyberSecurity Endpoint Detection and Response with extended functionality
Response actions
Network isolation of a device
IOC Scan
IOC file requirements
Extended telemetry for IOC Scan
IOC scan scope in the registry (RegistryItem)

- Running Critical Areas Scan
- Execution prevention
- Process start
- Terminate process
- Get file
- Delete file
- Move file to Quarantine
  - Viewing quarantined files
  - Sending a file from Quarantine to Kaspersky TIP
- Cloud Sandbox
- Working with alert details
  - About alert details
  - Viewing alert details
  - Applying and removing network isolation
  - Moving a file to Quarantine from alert details
  - Creating IOC Scan task from alert details
  - Preventing object execution from the alert details
  - Response actions for Active Directory users from alert details
    - Resetting the user password
    - Blocking a user account
    - Adding a user to a security group
    - Removing a user from a security group
  - Assigning Kaspersky ASAP training courses to users from alert details
- Monitoring & Reporting
  - Viewing the list of alerts
  - Viewing information about triggering of the Execution prevention rules
  - Viewing a list of isolated devices

Endpoint Agent mode
- Installing Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode
- Compatibility with third-party EPP applications

Managed Detection and Response
- Configuring MDR integration

Kaspersky Anti Targeted Attack Platform
- Configuring KATA integration
- Configuring telemetry

Endpoint Detection and Response Expert (on-premises)
- Configuring EDR Expert (on-premises) integration
- Configuring EDR Expert (on-premises) telemetry settings
- EDR Expert (on-premises) telemetry exclusions
- Exporting and importing EDR Expert (on-premises) event filters
- YARA Scan

EDR telemetry exclusions

Kaspersky Industrial CyberSecurity for Networks Integration
- Special considerations and limitations of the Kaspersky Industrial CyberSecurity for Networks integration
- Configuring Wi-Fi network monitoring

Monitoring EDR actions

- Kaspersky Endpoint Agent
  - Migrating the [KICS+KEA] configuration to [KICS+built-in Enpoint Agent] configuration
  - Migrating the policies and tasks of the [KICS+KEA] configuration to the [KICS+built-in agent] configuration
- SIEM Integration
  - Filtering events to be sent to SIEM
  - Exporting and importing telemetry event filtering rules
- Anomaly Detection using Sigma rules
  - Special considerations and limitations of Anomaly Detection using Sigma Rules
  - Enabling Anomaly Detection using Sigma Rules
  - Adding Sigma rules to a custom collection
  - Filtering Sigma rules within a collection of rules
  - Exporting and importing Sigma rules of a custom collection
  - Changing a Sigma rule
  - Exclusions in a Sigma rule
- Object isolation and backup
  - Isolating probably infected objects. Quarantine
    - Viewing quarantine objects
      - Sorting quarantined objects
      - Filtering quarantined objects
    - Restoring quarantined objects
    - Deleting objects from Quarantine
    - Sending probably infected objects to Kaspersky for analysis
    - Configuring Quarantine settings
  - Making backup copies of objects. Backup
    - Viewing objects in Backup
      - Sorting files in Backup
      - Filtering files in Backup
    - Restoring files from Backup
    - Deleting files from Backup
    - Configuring Backup settings
    - Backup statistics
  - Eliminating unprocessed threats
  - Blocking access to network resources. Blocked network sessions
    - List of blocked network sessions
    - Managing the list of blocked network sessions
- Event registration. Kaspersky Industrial CyberSecurity for Nodes logs
  - Ways to register Kaspersky Industrial CyberSecurity for Nodes events
  - Configuring the log settings
    - Sorting events in the log
    - Filtering events in the log
    - Deleting events from the log
    - Exporting information from the log
  - System audit log
  - Component and task logs
    - Viewing statistics and information about a Kaspersky Industrial CyberSecurity for Nodes task in task logs
  - Viewing the event log of Kaspersky Industrial CyberSecurity for Nodes in Event Viewer

- Administrator and user notification methods
  - Configuring administrator and user notifications
  - Configuring email notifications
- Configuring interaction with the Administration Server
- Configuring incident generation

Portable Auditor
- Hardware and software requirements
- Portable Auditor functionality limitations
- Creating Portable Auditor
- Updating Portable Auditor
- Working with the Portable Auditor Console
- Device scan
  - Malware Scan task settings
  - Security Audit task settings
  - Network traffic recording task settings
  - Importing and exporting task settings
- Viewing licensing information
- Viewing the scan results
  - Portable Auditor result files and their storage
  - Viewing the general Portable Auditor report
- Updating Portable Auditor databases
- Configuring Portable Auditor tracing and memory dump recording
- Working with the Portable Auditor Console using the command line
  - Exporting Portable Auditor results from a secure removable drive
- Blocking access to secure removable drives

Managing Kaspersky Industrial CyberSecurity for Nodes on the command line
- APPCONTROL. Importing Applications Launch Control rules
- APPCONTROL /CONFIG. Configuring the Applications Launch Control component
- APPCONTROL /GENERATE. Rule Generator for Applications Launch Control
- CONFIG. Supporting AM-PPL technology
- CREATEPORTABLE. Creating Portable Auditor
- DEVCONTROL. Importing Device Control rules
- DUMP. Recording memory dumps
- EDR_EXPERT_ON_PREM. EDR Expert (on-premises) integration
- EDRKATA. KATA Integration
- EXITPOLICY. Disabling policy on the device
- EXPORT. Exporting application settings
- FBRESET. Clearing iSwift base
- FIM /BASELINE. Baseline System Integrity Monitor
- HELP. Displaying command help
- IMPORT. Importing application settings
- KICS. Kaspersky Industrial CyberSecurity for Networks Integration
- ISOLATION. Managing Network isolation
- KSN. Using KSN/KPSN
- LICENSE. Application activation
- MDR. Configuring the Managed Detection and Response integration
- NETWORKBLOCKING. Managing Network Blocking

OMSINFO. Creating a JSON file with information about the application
PASSWORD. Password-protected access to Kaspersky Industrial CyberSecurity for Nodes functionality
PATCHCOMPATIBILITYRESET. Removing a patch from the list of incompatible patches
PERFANALYZER. Exporting Performance Analyzer task results
PREVENTION. Execution prevention
REMOTEACCESS. Managing Application Console remote connection settings
RESETMDRMACHINEID. Resetting device ID
RESTORE. Restoring files
ROLLBACK. Last update rollback
RTP. Real-Time File Protection
SCAN. On-Demand Scan
SCAN-IOC. IOC Scan
SCAN-OVAL. Security Audit
SCANCRITICAL. Critical Areas Scan
SERVERBINDINGDISABLE. Disabling Administration Server connection protection
SIEM. SIEM systems integration
SIGMA. Anomaly Detection using Sigma rules
START. Starting the application service
STARTPOLICY. Enabling policy
STOP. Stopping the application service
TASK. Managing tasks
TELEMETRYFILTERS. Exporting and importing telemetry event filtering rules
TOKEN. Managing access blocking to secure removable drives
TRACE. Tracing application operation
UPDATE. Updating databases and application software modules
YARA. Running YARA Scan
Contacting Technical Support
How to get technical support
Technical Support via Kaspersky CompanyAccount
Providing extended diagnostic information to Technical Support specialists
Tracing application operation
Contents and storage of trace files
Recording memory dumps
Protecting dump files and trace files
Obtaining OS data (Kaspersky Get System Info)
Sources of information about Kaspersky Industrial CyberSecurity for Nodes
Appendices
File extensions for quick scan
User accounts in application component rules
Legal Information
Data provision
Data provision under the End User License Agreement
Data provision when using Detection and Response solutions
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Industrial CyberSecurity for Networks Integration
SIEM Integration

Data provision when using Kaspersky Security Network
Compliance with European Union legislation (GDPR)
Information about third-party code
Trademark notices

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes is a comprehensive server and workstation security solution for IT threats in industrial control systems.

The application controls the operation of industrial enterprise network computers and uses the following components, functions, and technologies:

- **Applications Launch Control**. The component monitors user application starts and regulates application launches.
- **Device Control**. The component controls registration and usage of the external devices in order to protect computer against computer security threats, that may occur in process of file exchange with flash drives or other type of external device connected via USB.
- **PLC Project Integrity Check**. This function is designed to check the integrity of Programmable Logic Controller (PLC) projects used in an industrial system.

The operation of control components is based on rules, e.g.:

- Applications Launch Control uses applications launch control rules.
- Device Control uses device access rules and connector bus access rules.
- The PLC Project Integrity Check function uses PLC Project Integrity Check rules.

Each type of threat is handled by a separate component. Components can be enabled or disabled independently, and their settings can be configured.

The application checks and protects industrial network components using the following components:

- **Real-Time File Protection**. The component prevents the computer's file system from being infected. The component launches when Kaspersky Industrial CyberSecurity for Nodes starts, is continuously running in the computer's RAM, and checks all opened, saved, and started files on the computer and on all mounted drives. The Real-Time File Protection component observes each file event and checks this file for viruses and other programs that represent a threat.
- **Wi-Fi Control**. This component tracks a protected device's attempts to connect to Wi-Fi networks and blocks or allows connections to detected networks.
- **Firewall**. Depending on its mode, the component: monitors traffic filtering by Windows Firewall; only records events about network activity of the protected computer in the component's log; or filters network traffic according to the Firewall settings.
- **Anti-Cryptor** This component makes it possible to detect malicious encrypting of the network file resources of a protected device from remote computers on the corporate network.
- **Portable Auditor**. This component examines the isolated devices and performs the security inspection.
- **BadUSB Attack Prevention**. The component prevents infected USB devices emulating a keyboard from connecting to the computer.

- **File Integrity Monitor**. Kaspersky Industrial CyberSecurity for Nodes detects changes in files within the monitoring scopes specified in the task settings. These changes may indicate a security breach on the protected device.

- **Registry Access Monitor**. This component makes it possible to monitor actions performed with the specified registry branches and keys in the monitoring scopes defined in the task settings.

- **Log Inspection**. This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.

In addition to the real-time protection provided by the components, we recommend that a regular scan of the computer be run to check for viruses and other applications that could pose a threat. This should be done to prevent the spread of any malware that was not detected by the components, e.g. due to a low level of protection in the settings or for other reasons.

To keep Kaspersky Industrial CyberSecurity for Nodes operating properly, databases and software modules utilized during the program's operation should be updated. By default, the application automatically updates, but, if required, you may manually update the application databases and modules.

The following tasks are used to protect computers:

- **Full Scan**. Kaspersky Industrial CyberSecurity for Nodes carefully checks the operating system, including system memory, any objects booted at operating system start, and the backup of the operating system, as well as all hard and removable drives.

- **Custom Scan**. Kaspersky Industrial CyberSecurity for Nodes scans user-selected objects.

- **Critical Areas Scan**. Kaspersky Industrial CyberSecurity for Nodes scans objects that are loaded at operating system start, are in system memory, or are objects that may contain rootkits.

- **Update**. Kaspersky Industrial CyberSecurity for Nodes downloads application database and module updates. Updates help the computer's protection stay up to date against viruses and other programs that pose a threat.

Remote Access through Kaspersky Security Center

Kaspersky Security Center allows Kaspersky Industrial CyberSecurity for Nodes to be started and stopped, for tasks to be administered, and program settings to be adjusted remotely on a client computer.

Application Utilities

Kaspersky Industrial CyberSecurity for Nodes contains an array of utilities. Utilities are designed to keep the application up to date and expand the application's ability to provide assistance.

- **Logs**. The activity of each component and task is recorded in a log during the application's operation. The log is a list of events that occurred during the operation of Kaspersky Industrial CyberSecurity for Nodes, as well as all operations undertaken by the application. If a problem occurs, logs may be sent to Kaspersky for Technical Support specialists to analyze.

- **Storages**. If during a scan for viruses and other programs that pose a threat the application detects an infected or probably infected file on a computer, it blocks this file. Probably infected files will be transferred by Kaspersky Industrial CyberSecurity for Nodes to Quarantine, a specialized storage. Kaspersky Industrial CyberSecurity for Nodes saves copies of the disinfected and deleted files to Backup. Kaspersky Industrial CyberSecurity for Nodes puts files that have not been processed for any reason into the list of unprocessed files. You can scan files, restore files to their original folder, manually quarantine files, and clear the data storage.

- **Notifications**. The notifications service allows the user to be updated about events, the current status of the computer, and the operation of Kaspersky Industrial CyberSecurity for Nodes. Notifications may be displayed on screen or sent via email.

- **Kaspersky Security Network**. User participation in the Kaspersky Security Network (KSN) permits improved computer protection by allowing the system to receive information on file reputation, web resources, and software that is received from users all over the world in real time.

- **Exploit Prevention** You can protect process memory from exploits using a Protection Agent injected into the process.

- **List of blocked network sessions**. You can block network sessions that try to access the computer's shared network folders if any malicious activity is detected on their side.

- **Trusted Zone**. You can create a list of exclusions from the protection or scan scope that Kaspersky Industrial CyberSecurity for Nodes will use by default in On-Demand Scan and Real-Time File Protection tasks and in other tasks if you specify them in the exclusion settings.

- **Support**. All registered Kaspersky Industrial CyberSecurity for Nodes users receive access to application database and module updates, as well as consultations with Kaspersky Technical Support specialists via email on any question related to installation, configuration, and use of the application.

What's new

Update 5.0

Kaspersky Industrial CyberSecurity for Nodes 5.0 introduces the following features and improvements:

- The application collects information about user sessions to enhance the level of User Account Control on protected devices using Kaspersky Industrial CyberSecurity for Networks. User session monitoring is available in Kaspersky Industrial CyberSecurity for Networks version 5.0 and later. For more details, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

- You can now collect and send to Kaspersky Industrial CyberSecurity for Networks data about Wi-Fi networks detected by a protected device with the application installed, as well as data about devices connected to the same Wi-Fi network as the protected device. Wi-Fi network monitoring is available in Kaspersky Industrial CyberSecurity for Networks version 5.0 and later. For more details, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

- For Kaspersky Industrial CyberSecurity for Networks users, the following new response actions are added: *Delete file*, *Run process, Terminate process*, *Block user*, *Unblock user*, *Terminate user session*, *Reset user password*, *Block connections*. The specified response actions are available in Kaspersky Industrial CyberSecurity for Networks version 5.0 and later. For more details, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

- Portable Scanner has been renamed to Portable Auditor. The component also includes the following changes:

  - Added a full graphical user interface to manage Portable Auditor.

  - Added support for Rutoken EDS 3.0 Flash for creating a Portable Auditor.

  - Increased the execution speed of Portable Auditor tasks with the default settings.

- You can now configure the scheduled tasks to run only on specified days of the week at a specified interval in weeks. The schedule is available in Kaspersky Security Center 16.1 or later.

- You can now pause On-Demand Scan tasks for a selected time interval, for example, to perform routine maintenance.

- Performance of the hard drive subsystem on the protected device has been optimized by reducing the number of I/O operations.

- The application can now run on devices with older processors: Celeron III and VIA C3.

- The Anomaly Detection using Sigma rules component now includes the Audit of file sharing over a network and via removable media predefined rule collection. The collection allows you to log events related to reading, writing, and deleting files in network folders, as well as copying files to removable media on the local node.

- The TREI-5B controller is now supported for the *PLC Projects Integrity Check* task.

- The following operating systems are now supported:
  - Windows 11 26H2
  - Windows 11 IoT 25H2
  - Windows Server 2025
- Token-based authentication for domain accounts is now supported in the Application Console. Now, to access the application functions, you can use either your user name and password or a token or smart card.
- New telemetry events are now available to users of Kaspersky Endpoint Detection and Response. These new events enhance the threat detection capabilities using Kaspersky EDR solutions.
- Fixed the application's behavior when starting the *Security Audit* task with rule sets containing unsupported types of OVAL checks. Now, when unsupported types of OVAL checks are detected, the application does not interrupt task execution, and information about unsupported checks is displayed as errors in the report.
- Extended policy audit is supported in Kaspersky Security Center Web Console version 15.0 or later. Now you can view policy revisions and save them to a file. For more details about working with revisions, refer to the Kaspersky Security Center Help.
- The *Operation with the device is prohibited until Kaspersky Industrial CyberSecurity for Nodes startup* and *Device connection is blocked until Kaspersky Industrial CyberSecurity for Nodes startup* events are now available. Now, if the device is blocked before the application is launched, the corresponding event will be generated and sent to the Administration Server.
- The default interval for sending synchronization requests to the Kaspersky Industrial CyberSecurity for Networks server is now 1 minute instead of 5 minutes.
- When developing this version of Kaspersky Industrial CyberSecurity for Nodes, we incorporated the changes included in the following private patches: PF23040, PF23051, PF23065, PF23087, PF23100, PF23106.

Update 4.5

The following new features and improvements are implemented in Kaspersky Industrial CyberSecurity for Nodes 4.5:

- Significantly updated user interface of the Application Console and the plug-ins for managing the application using Kaspersky Security Center.
- Support for Windows 11 24H2.
- Now you can change the port that the Application Console uses to connect to a computer with the application installed.

- In the *Trusted zone*, you can:
  - Edit exclusion profiles for industrial applications when installing the application and creating an application management policy using Kaspersky Security Center.
  - Configure trusted processes in a more granular way.
  - Use the trusted certificate store.
- New settings for user and group rights to manage the application.
- New *Anti-Rootkit* component. By default, the component is enabled if Real-Time File Protection is enabled. You can disable the component while installing the application, using the Change application components of Kaspersky Industrial CyberSecurity for Nodes task, or in the properties of the application installation package.
- In *Exploit Prevention* settings, the application can now automatically identify protected processes.
- New *Remediation Engine* component.
- The *Anti-Cryptor* component monitors shared folders as well as local folders.
- Reworked *Applications Launch Control* component:
  - Significant changes in the structure of component settings.
  - To specify Applications Launch Control rule triggering conditions and exclusions, you can now use the drive type, KL categories, KSN groups.
- Reworked *Device Control* component:
  - By default, the *Device Control* component is configured to allow connection of all devices.
  - *Wi-Fi Control* is no longer a separate component and is now part of Device Control.
  - The possibility to control connected devices depending on the connection bus has been added.
  - Migration of settings for access to removable drives when upgrading from previous versions of the application to version 4.3 has been added.
- The *Firewall Management* component has been reworked into the *Firewall* component, which, in addition to interfacing with the Windows firewall, now additionally functions as a firewall.
- The functionality of the *File Integrity Monitor* and *Registry Access Monitoring* components has been merged into the new *System Integrity Monitoring* component. This improvement lets you efficiently track changes in the file system and Windows registry, increasing the protection against unauthorized modification of data.
- Kaspersky Endpoint Agent functionality is now integrated into the application as the built-in Endpoint Agent (Detection and Response).
- The configuration of events for sending to SIEM has been expanded. Now Kaspersky Industrial CyberSecurity for Nodes supports sending Windows Event Log events.
- The application does not support scheduling individual components. If the components are enabled, they keep running while the application is running.
- Kaspersky Security Center Windows 15.1 is now supported.

- Group tasks added:
  - To implement the functionality of Kaspersky Endpoint Agent: Security Audit, Run process, Terminate process, IOC Scan, Get file, Move file to Quarantine, Delete file.
  - Other tasks:
    - Administration Server connection protection
    - Change Kaspersky Industrial CyberSecurity for Nodes components
    - Baseline System Integrity Monitor instead of Baseline File Integrity Monitor
    - Update instead of Copying Updates, Application Database Update and Software Modules Update
    - Update rollback instead of Rollback of Application Database Update
    - Remove key
- Network communication events of level L2 sent to Kaspersky Industrial CyberSecurity for Networks now include the IPv4 address of the network interface through which the traffic passes (the adapter.address field).
- Facilitated integration with Kaspersky Industrial CyberSecurity for Networks solution. Starting with version 4.5 of Kaspersky Industrial CyberSecurity for Nodes, the following types of configurations are supported:
  - ARP table
  - routing table
  - password policy
  - security audit policy
  - extended audit policy
- Kaspersky Industrial CyberSecurity for Networks integration settings now allow configuring the promiscuous mode for the application and network interfaces of the host that allows sending extended telemetry to Kaspersky Industrial CyberSecurity for Networks.
- Information about file operations (reading, writing, deletion) in shared folders and on devices connected to the local host can now be sent to the Kaspersky Industrial CyberSecurity for Networks server. To get information about file operations, you need a collection of corresponding Sigma rules. Kaspersky Industrial CyberSecurity for Networks can use the received information to detect instances of files being copied between network shares of computers running Kaspersky Industrial CyberSecurity for Nodes, or files being copied from network shares to devices connected to computers running Kaspersky Industrial CyberSecurity for Nodes.
- In Kaspersky Security Center Web Console, in the properties of the host on which the application is installed, in the Detection and Response section, you can now view the threat response history of Kaspersky Industrial CyberSecurity for Nodes together with the response history of other solutions that are managing the host.

- The following features and improvements are available to users of Endpoint Detection and Response (EDR) solutions by Kaspersky.
  - Filling in alert details with new data. Now the alert details contain more information about the threat, including how the application behaves when responding to EDR threats.
  - Now you can manage Network Isolation in alert details. Additionally, in the alert details you can specify the computer Network Isolation time period and add exclusions.
  - The IOC files processing has been improved. Now you can view and edit the contents of IOC files in the interface of Kaspersky Security Center Web Console. After loading an IOC file, the application displays a report on the IOC terms application.
  - Improved response to detected IOCs. Now you can quarantine files detected by the *IOC Scan* task directly in IOC detection results in task properties. You can also isolate computers from the network in the task properties.
  - Now you can create IOC files directly in the properties of the *IOC Scan* task based on lists of file hashes, IP addresses, or DNS names generated in a TXT file.
  - Expanded scan scope for the *IOC Scan* task. Now you can define a scope for the IOC Scan of the registry (**Windows Registry – RegistryItem**). In earlier versions of the application, you could only use a predefined IOC Scan scope in the registry.
- The *Network Threat Protection* component can monitor network traffic to detect port scanning and high-intensity network requests.
- In the Application console, in the **Telemetry collection servers** section, you can now configure the following integrations:
  - Integration with Kaspersky Endpoint Detection and Response Expert (on-premise)
  - Integration with KICS for Networks
  - SIEM Integration
- As part of the integration with KICS for Networks, you can send telemetry to an MQTT broker server built into a software data diode.
- Support for Allen-Bradley ControlLogix PLCs has been added to the *PLC Project Integrity Check* task.
- Introducing the *Performance Analyzer*. Performance Analyzer is a task that collects and analyzes information about access to files and applications on the device. This information can help you define a trusted zone to minimize the impact of the application on the performance of industrial software.
- For the Anomaly Detection using Sigma rules component, the following new collections are now available:
  - *Collection of user activity monitoring rules using Windows logs*. This collection allows registering events when new users are added, user privileges are elevated, users log in to the system and others.
  - *Collection of rules for the detection of suspicious activity when using SIMATIC PCS7, Siemens STEP7, Siemens TIA Portal, Siemens WinCC software*.
  - *Collection of rules for the detection of suspicious activity when using Yokogawa CENTUM VP, ProSafe-RS systems*.

- The application checks the configuration of control components before saving the settings. The check was added for the Applications Launch Control, Device Control, System Integrity Monitoring components. The application now displays a warning if the current settings of the control component may increase the load on the computer or cause system failures. For example, in the case of Applications Launch Control, if you selected the mode that blocks all applications except allowed ones, and you did not add any allow rule, the application displays a warning because such a configuration may cause system failures.

- Added new components:

  - *Managed Detection and Response for ICS*. This component facilitates interaction with the solution known as Kaspersky Managed Detection and Response for Industrial Control Systems. The *Kaspersky Managed Detection and Response (MDR)* solution automatically detects and analyzes security incidents in the industrial infrastructure. To do so, MDR uses telemetry data received from endpoints and machine learning. MDR sends incident data to Kaspersky experts. The experts can then process the incident and, for example, add a new entry to Anti-Virus databases.

  - *BadUSB Attack Prevention*. The BadUSB Attack Prevention component prevents infected USB devices emulating a keyboard from connecting to the computer. When an USB device that the operating system identifies as a keyboard is connected to the computer, the application prompts the user to type a code on this keyboard to authorize the keyboard.

  - *BitLocker Full Disk Encryption*. BitLocker is an encryption technology built into Windows operating systems. Kaspersky Industrial CyberSecurity for Nodes allows you to control and manage Bitlocker using Kaspersky Security Center.

- Support of the *OPC UA* protocol for sending data to a SCADA system through the Kaspersky Security Gateway. In addition to the IEC 60870-5-104 and OPC DA protocols, the application now supports the OPC UA protocol, providing cross-platform compatibility.

- Windows XP and Windows XP SP1 support for the Portable Scanner. The Portable Scanner can scan isolated devices for viruses and other threats.

- The *PLC Project Investigation* task now supports authentication on Siemens SIMATIC S7-1200 / 1500 controllers. Now you can enter a password for the connections to these PLC models in the task properties.

Fixed issues

The table below lists all issues discovered in previous versions of Kaspersky Industrial CyberSecurity for Nodes and fixed in the current version.

List of issues fixed in version 5.0

Identifier	Issue Description
9527176	In the Web Console, it is not possible to import Firewall rules previously exported from the Application Console into a policy.
9986614	In the Web Console and the Kaspersky Security Center Administration Console, it is not possible to import a list of trusted devices from a TXT file containing a selection of Kaspersky Security Center events related to blocked devices, which was exported from the Web Console.
10094028	When creating a Portable Auditor, the Audit configuration sample profile is incorrectly displayed in the list of compliance and security configurations for operating systems.

Identifier	Issue Description
10700703	In the interface of the System Integrity Monitoring, Trusted zone, Applications Launch Control, and Device Control components, it is not immediately clear how to select list items to execute the **Export selected** command. The description in the application help has been expanded.
10720231	The trusted devices counter is not displayed in the **Device Control** section of the policy in the Kaspersky Security Center Administration Console.
10729552	Events related to file operations on removable drives are not being generated, even though logging for such events is enabled.
10752491	In the Web Console, it is not possible to import a list of trusted devices from a TXT file containing a selection of Kaspersky Security Center events related to blocked devices, which was exported from the Administration Console.
10753980	As a result of running the *Malware Scan* task, Portable Auditor incorrectly creates a KLQ file instead of a password-protected ZIP archive.

Distribution kit

The distribution kit includes the welcome application that lets you do the following:

- Start the Kaspersky Industrial CyberSecurity for Nodes application Installation Wizard.
- Start the Kaspersky Industrial CyberSecurity for Nodes Console Installation Wizard.
- Start Kaspersky Virus Removal Tool.
- Start the Kaspersky Security Gateway setup.
- Read about this version of Kaspersky Industrial CyberSecurity for Nodes.
- Open the Kaspersky Industrial CyberSecurity for Nodes 5.0 Help.
- Open the Kaspersky Industrial CyberSecurity Endpoint Detection and Response Help.
- Go to Kaspersky Industrial CyberSecurity for Nodes page on the Kaspersky website.
- Visit the Kaspersky website.
- Visit the Technical Support website.

The distribution kit files are stored in the different folders depending on their intended use (see table below).

Kaspersky Industrial CyberSecurity for Nodes distribution kit files

File	Purpose
autorun.inf	Autorun file for the Kaspersky Industrial CyberSecurity for Nodes Installation Wizard when installing the application from removable drive.
setupui.exe	Application welcome screen launch file.
kics_win.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of the application via Kaspersky Security Center.
\client\kicstools.msi	Windows Installer installation package; installs Kaspersky Industrial CyberSecurity for Nodes Console on the protected devices.
\client\setup_kicstool.exe	The file that starts the wizard for installing the Kaspersky Industrial CyberSecurity for Nodes Console. The installation package file kicstools.msi is started with the installation settings specified in the wizard.
\client\license.txt	Kaspersky Industrial CyberSecurity for Nodes Management Console End User License Agreement and Privacy Policy text file.

File	Purpose
\exec\bases.cab	Archive of anti-virus databases current at the time of application release.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Files for removing incompatible software.
\exec\incompatible.txt	Kaspersky does not guarantee the compatibility of Kaspersky Industrial CyberSecurity for Nodes with applications listed in the file.
\exec\installer.ini	File that contains the internal settings of the distribution kit.
\exec\kics.cab	Files for the graphical interface of the application.
\exec\kics_win.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of the application via Kaspersky Security Center.
\exec\kics_win.msi	Windows Installer installation package: this installs Kaspersky Industrial CyberSecurity for Nodes on the protected device.
\exec\klcfginst.msi	Installer for Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in available via the Kaspersky Security Center. Install the Administration Plug-in on each protected device where the Kaspersky Security Center Administration Console is installed if you plan to use it for managing Kaspersky Industrial CyberSecurity for Nodes.
\exec\ksn_en.txt	File with the text of the KSN Statement.
\exec\license.txt	Kaspersky Industrial CyberSecurity for Nodes End User License Agreement and Privacy Policy text file.
\exec\package.kcat	File with the signatures of distribution kit files.
\exec\setup_kics.exe	The file that starts the wizard for installing Kaspersky Industrial CyberSecurity for Nodes on the protected device; it starts the installer package file kics_win.msi with the installation settings specified in the wizard.
\gateway\security_gateway.msi	Windows Installer installation package; installs Kaspersky Security Gateway.
\gateway\opc_redist.msi	Windows Installer service installation package; installs OPC Core Components Redistributables.
\gateway\license.txt	Kaspersky Security Gateway End User License Agreement and Privacy Policy text file.
\kvrt\KVRT.exe	Installer for Kaspersky Virus Removal Tool.
\setup\images	Folder with application welcome screen launch files.
\setup\setup.hta	Application welcome screen launch file.
\setup\SETUP_STRINGS.JS	File with the application string resources.

Distribution kit files can be run from the Installation CD. If you have copied the distribution package files onto the local drive beforehand, make sure that the structure of the distribution kit files has been preserved.

Hardware and software requirements

Software requirements for the protected device

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Windows Installer 3.1 is required for proper installation and operation of the application on a protected device running Microsoft Windows XP.

To install and use Kaspersky Industrial CyberSecurity for Nodes on protected devices with embedded operating systems, the Filter Manager component (Filter Manager) is required.

For correct operation of Kaspersky Industrial CyberSecurity for Nodes, SHA-2 support in Microsoft Windows is required. For detailed information, see knowledge base on the Technical Support website.

You can install Kaspersky Industrial CyberSecurity for Nodes on a device running one of the following 32-bit or 64-bit Microsoft Windows operating systems:

Desktop operating systems:

- Windows XP Professional SP2 32-bit / 64-bit
- Windows XP Professional SP3 32-bit
- Windows Vista SP2 32-bit / 64-bit
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32-bit / 64-bit
- Windows 8 Pro / Enterprise 32-bit / 64-bit
- Windows 8.1 Pro / Enterprise 32-bit / 64-bit
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit

- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit

Server operating systems:

- Windows Server 2003 SP1 Standard / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-bit
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2008 SP2 Standard / Enterprise 64-bit
- Windows Small Business Server 2011 Essentials / Standard 64-bit
- Windows MultiPoint Server 2011 64-bit
- Windows Server 2012 Foundation / Essentials / Standard 64-bit
- Windows Server 2012 R2 Foundation / Essentials / Standard 64-bit
- Windows Server 2016 Essentials / Standard 64-bit
- Windows Server 2019 RS5 Essentials / Standard 64-bit
- Windows Server 2022 21H2 64-bit

- Windows Server 2022 version 20348.350 64-bit
- Windows Server 2025 version 26100.1742 64-bit

Embedded systems:

- Windows XP Embedded Service Pack 3 32-bit
- Windows Embedded POSReady 7 32-bit / 64-bit
- Windows Embedded Standard 7 Service Pack 1 32-bit / 64-bit
- Windows Embedded 8 Standard 32-bit / 64-bit
- Windows Embedded 8.1 Industry Pro 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1507 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1607 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1803 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1809 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1903 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 2004 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 20H2 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 21H1 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 21H2 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 22H2 32-bit / 64-bit
- Windows 11 IoT Enterprise Version 21H2 64-bit
- Windows 11 IoT Enterprise Version 22H2 64-bit
- Windows 11 IoT Enterprise Version 23H2 64-bit
- Windows 11 IoT Enterprise Version 24H2 64-bit
- Windows 11 IoT Enterprise Version 25H2 64-bit

Hardware requirements for the protected device

Hardware requirements for the protected device

OS type	OS name	Minimum requirements	Recommended requirements
Workstations	Windows XP x86	• Processor: 1 GHz single-core processor, Celeron III or higher, or VIA C3 • RAM: 256 MB • Free disk space: 2GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
	Windows XP x64 Windows 7 / 8 x86	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher • RAM: 256 MB • Free disk space: 2GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
	Windows 7 / 8 / 10 / 11 x64	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher • RAM: 256 MB • Free disk space: 2GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
For servers	Windows Server 2003 x86/x64 Windows Server 2008 x86	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher • RAM: 256 MB • Free disk space: 4GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64 Windows Server 2022 x64	• Processor: 1.4 GHz single-core • RAM: 256 MB • Free disk space: 4GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
Embedded	Windows Embedded XP	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher • RAM: 256 MB • Free disk space: 2GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB
	Windows 7 / 8 / 10 Embedded	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher • RAM: 256 MB • Free disk space: 2GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB • Free disk space: 4GB

Supported industrial systems

Kaspersky Industrial CyberSecurity for Nodes 5.0 protects the following programmable logic controllers:

- Siemens™ SIMATIC™ S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-400H
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIPROTEC 4
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580

- devices based on CODESYS V3
- OWEN PLC210
- Fastwel CPM723-01
- Prosoft Systems Regul R500
- Emerson DeltaV
- Rockwell Automation Allen-Bradley ControlLogix
- TREI-5B

Hardware and software requirements for Kaspersky Security Gateway

General hardware and software requirements:

- 1 GB of free disk space
- The Kaspersky Security Center Administration Server must be installed if the klakaut service is selected as a data provider

Desktop operating systems:

- Windows 7 SP1 Pro / Enterprise / Ultimate 32-bit / 64-bit
- Windows 8 Pro / Enterprise 32-bit / 64-bit
- Windows 8.1 Pro / Enterprise 32-bit / 64-bit
- Windows 10 LTSC 2015 version 1507 32-bit / 64-bit
- Windows 10 LTSC 2016 version 1607 32-bit / 64-bit
- Windows 10 RS4 version 1803 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 version 1809 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 LTSC 2019 version 1809 32-bit / 64-bit
- Windows 10 19H1 version 1903 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 version 2004 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H2 version 2009 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H1 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 LTSC 2021 version 21H2 32-bit / 64-bit
- Windows 10 22H2 Home / Pro / Education / Enterprise 32-bit / 64-bit

- Windows 11 23H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 22H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 21H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 22H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 23H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 24H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 25H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 26H2 Home / Pro / Education / Enterprise 64-bit

Server operating systems:

- Windows Server 2008 R2 Standard / Enterprise 32-bit / 64-bit
- Windows Server 2008 SP1 R2 Standard / Enterprise 32-bit / 64-bit
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter 64-bit
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit
- Windows Server 2022 21H2 64-bit
- Windows Server 2022 version 20348.350 64-bit
- Windows Server 2025 version 26100.1742 64-bit

Supported versions of Kaspersky Security Center

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

- Kaspersky Security Center Linux versions 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3, 17.0. Management of Kaspersky Industrial CyberSecurity for Nodes is supported via Kaspersky Security Center Web Console.
- Kaspersky Security Center Windows version 15.1. Management of Kaspersky Industrial CyberSecurity for Nodes is supported via Kaspersky Security Center Administration Console and via Kaspersky Security Center Web Console.

- Kaspersky Security Center Windows 14.0. Management of Kaspersky Industrial CyberSecurity for Nodes installed on devices running the Microsoft Windows XP SP3 operating system is supported via Kaspersky Security Center Administration Console and via Kaspersky Security Center Web Console.

- Kaspersky Security Center Windows 10.5. Management of Kaspersky Industrial CyberSecurity for Nodes installed on devices running the Microsoft Windows XP SP2 operating system is supported via Kaspersky Security Center Administration Console and via Kaspersky Security Center Web Console.

To manage Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center, Kaspersky Security Center Network Agent is required.

Kaspersky Security Center Network Agent is not included in the Kaspersky Industrial CyberSecurity for Nodes distribution kit. You can download it on the applications download page in the **Kaspersky Security Center** section.

Kaspersky Virus Removal Tool

Kaspersky Virus Removal Tool is a utility designed to check and disinfect infected computers running Microsoft Windows operating systems. Kaspersky Virus Removal Tool detects viruses, Trojans, and other programs threatening the protected device, and lets users select how detected infected objects should be handled.

Kaspersky Virus Removal Tool does not require installation. The application may be started in the following manner:

- From the kvrt\ folder, start the kvrt.exe executable file included in the Kaspersky Industrial CyberSecurity for Nodes 5.0 distribution kit.

- Click the **Run Kaspersky Virus Removal Tool** link in the welcome window.

The utility cannot be started through the local Console or Administration Plug-in of Kaspersky Industrial CyberSecurity for Nodes 5.0.

After disinfecting any detected infection, the computer must be restarted. We recommend running Kaspersky Virus Removal Tool only during technological windows in the industrial network operation.

Kaspersky Virus Removal Tool is not part of the Kaspersky Industrial CyberSecurity for Nodes solution and does not depend on application components.

Anti-virus database updates are performed independently of Kaspersky Industrial CyberSecurity for Nodes 5.0 updates. When starting Kaspersky Virus Removal Tool, the application will inform you if an update is required. To update the utility, you must be connected to the Internet.

The operation of Kaspersky Virus Removal Tool is governed by a separate End User License Agreement that you may read on the technical support site.

The technical support site also provides information about system requirements for the computer where the utility is started, and detailed instructions on working with Kaspersky Virus Removal Tool.

Functional requirements and limitations

This section describes additional functional requirements and existing limitations for Kaspersky Industrial CyberSecurity for Nodes components.

Installing and removing the application

- For correct operation of Kaspersky Industrial CyberSecurity for Nodes, SHA-2 support in Microsoft Windows is required.
- When you install the application, a warning may appear on the screen If the specified path to the Kaspersky Industrial CyberSecurity for Nodes installation folder contains more than 150 characters. The warning does not affect the installation process: you can install and run Kaspersky Industrial CyberSecurity for Nodes.
- If you want to install the SNMP protocol support component, make sure to restart the SNMP service if the SNMP service is running.
- If you want to install and run Kaspersky Industrial CyberSecurity for Nodes on a device running on an embedded operating system, make sure to install the Filter Manager component.
- You cannot install Administration Tools via Microsoft Active Directory® group policies.
- If you exclude the Anti-virus Protection node from the list of installed application components, this node disappears from the list of available components after the installation is completed. To install the components of the Anti-virus Protection node, start the Installation Wizard from the installation package since the installation package contains a full list of components.
- If Kaspersky Industrial CyberSecurity for Nodes Administration Console is installed, the Installation Wizard may prompt to restart the computer. In this case, reboot is not mandatory. It is sufficient to end the session of the user who installed the Administration Console and log in to the system again.
- When installing the application on a Windows XP or Windows Vista device, you may need to install the DigiCert Assured ID Root CA certificate to enable driver signature verification. If necessary, this certificate will be automatically installed into the trusted root certificate store of the operating system from the installation package of the application.
- When installing the application on Windows XP or Windows Vista devices, you need to check if the DigiCert High Assurance EV Root CA. is present.

  If this root certificate is not installed, the application may function improperly. We recommend that you install the certificate as soon as possible.
- Application installation finishes with an error if the path to the installation folder is the same as the path to at least one of the following folders: application database folder, Backup folder, folder for restoring objects from Quarantine, temporary file folder.
- If you manage Kaspersky Industrial CyberSecurity for Nodes using Kaspersky Security Center Cloud Console, updating the application locally is not allowed. When updating the application locally, it is not possible to accept the Data Processing Agreement for Kaspersky Security Center Cloud Console.

System Integrity Monitoring

By default, the System Integrity Monitoring component does not monitor changes in the system folders or the file system's housekeeping files to not clutter task reports with information about routine file changes performed constantly by the operating system. You cannot include such folders in the monitoring scope.

The following folders and files are excluded from the monitoring scope:

- NTFS housekeeping files with file id from 0 to 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\

The application excludes top-level folders.

The component does not monitor files changes that bypass the ReFS/NTFS file system (file changes made through BIOS, LiveCD, and more).

Firewall

- You should specify more than one address. Otherwise, working with IPv6 is unavailable.
- Preset Firewall rules support basic scenarios of interaction between protected devices and Administration Server. To make full use of Kaspersky Security Center functions, you need to configure port rules. You can find information about port numbers, protocols and their functions in the Kaspersky Security Center Knowledge Base.
- After the application is installed and Firewall rules are configured, the application monitors changes to Windows Firewall rules and rule groups when the Firewall component is running. To update the status and to add necessary Windows Firewall rules, restart the Firewall component.
- When you start the Firewall component, the deny rules and rules that control outbound traffic are automatically removed from Windows Firewall settings.
- Characters `*` and `?` cannot be used in the application path and in the name of the Firewall rule for applications.
- If the *Observe the state of Windows Firewall* mode is selected, the Windows Firewall settings (**Settings** → **Update & Security** → **Windows Security** → **Firewall & network protection**) will show that the Kaspersky Industrial CyberSecurity for Nodes Firewall is disabled. If you click the button that enables the Firewall, its operating mode changes to *Block*.
- On computers running Windows 7 and Windows Server 2008 R2, Firewall rules configured for the TermService service based on the service name do not restrict access via RDP.
- When the Firewall is running in the **Block** mode, the application prevents obtaining an IP address from the DHCP server. To obtain an IP address, configure the Firewall to allow the svchost.exe system process.

Limitations on outdated Windows versions

- Windows XP SP2 version do not allow blocking remote devices and configure the List of blocked network sessions settings. In this Windows version, the **Block access to network shared resources for the sessions that show malicious activity** option is inactive.
- Kaspersky Industrial CyberSecurity for Nodes installation:
  - On computers running Windows XP SP2 Professional (32-bit/64-bit), Windows Server 2003, or Windows Server 2003 R2, when installing the application using Kaspersky Security Center, you must place the setup.exe file from the Network Agent 10.5.1781 installation package into the application installation package folder, and install a private patch for Kaspersky Security Center.
  - On computers running Windows XP SP3 Professional (32-bit), or Windows XP Embedded SP3 (32-bit), when installing the application using Kaspersky Security Center, you must place the setup.exe file from the Network Agent 14.0.0.20023 installation package into the application installation package folder, and install a private patch for Kaspersky Security Center.

    For the necessary files and instructions, please contact Technical Support.

- To manage Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center:
  - on a computer running Windows XP SP2 Professional (32-bit/64-bit), Windows Server 2003 or Windows Server 2003 R2, you must use Kaspersky Security Center Network Agent version 10.5.1781.
  - on a computer running Windows XP SP3 Professional (32-bit) and Windows XP Embedded SP3 (32-bit), you must use Kaspersky Security Center Network Agent version 14.0.0.20023.
- On Windows XP computers, telemetry cannot be sent to a data diode using the MQTT protocol.
- For the *Performance Analyzer* task to work correctly, the computer on which the task is started must be running Windows Vista or later.

Integration with Kaspersky Security Center

- When update packages are received, Administration Server verifies database updates before sending the updates to protected devices on the network. Kaspersky Security Center Administration Server does not verify application module updates.
- Make sure that the required check boxes are selected in the Interaction with the Kaspersky Security Center Administration Server settings when you use the components that transmit dynamic data to Kaspersky Security Center using network lists (Quarantine, Backup).
- Network Agent 10.5 does not send information about installed components to the Kaspersky Security Center Administration Server. For this reason, in Kaspersky Security Center Administration Console and Kaspersky Security Center Web Console, the settings of a device with Network Agent 10.5 do not display installed Kaspersky Industrial CyberSecurity for Nodes components and their settings.
- If Kaspersky Security Center Network Agent 10.5 is installed on the device, you cannot use Kaspersky Security Center Web Console to download files in Backup.
- If Kaspersky Industrial CyberSecurity for Nodes is installed with enabled low resource consumption mode for Kaspersky Security Center Network Agent (default, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) and then the Network Agent is installed, Kaspersky Industrial CyberSecurity for Nodes does not create an exclusion for the Network Agent in Windows Firewall, therefore Windows Firewall blocks the Network Agent.
- If Kaspersky Industrial CyberSecurity for Nodes is installed with enabled low resource consumption mode for Kaspersky Security Center Network Agent (default, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), modifications of network lists are reflected in the Kaspersky Security Center Administration Console with a delay of approximately ten minutes.
- When searching for managed devices in the Kaspersky Security Center Administration Console, the **Application components** tab may simultaneously display multiple variants of the name of the same application component, including names corresponding to older versions of Kaspersky Industrial CyberSecurity for Nodes. The names of some components may also be duplicated.

  To search by component, you simply need to select one of the displayed variants. For more details on device discovery, refer to the Kaspersky Security Center Help.

Other limitations

On-Demand Scan and Real-Time File Protection

- Scanning of connected MTP-devices is not available.
- Archive scanning is unavailable without SFX-archive scanning: if archive scanning is enabled in the protection settings of Kaspersky Industrial CyberSecurity for Nodes, the application automatically scans objects in both archives and SFX-archives. SFX-archive scanning is available without archive scanning.
- If **Deep analysis of launching processes (process launch is blocked for the duration of analysis)** checkbox and **KSN Usage** are enabled simultaneously, any launched process that receives URL web-address as an argument will be blocked, even if the "Inform" mode was chosen. To avoid blocking the process, please choose one of the options:
  - Disable **KSN Usage**.
  - Disable **Deep analysis of launching processes (process launch is blocked for the duration of analysis)** checkbox

  Recommended option: clear the **Deep analysis of launching processes (process launch is blocked for the duration of analysis)** check box.

Licensing

- You cannot activate the application with a key via the Setup wizard if the key was created using the SUBST command, or if the path to the key file is a network path.
- If you plan to use a Kaspersky Security Center proxy server to activate the product on a client device, disable VDI optimization on that device when installing Kaspersky Security Center Network Agent.

Update

- During the installation and uninstallation of Kaspersky Industrial CyberSecurity for Nodes patches installed on Windows XP devices, due to the peculiarities of this operating system, the device may need to be restarted.
- By default, the application icon is hidden after Kaspersky Industrial CyberSecurity for Nodes critical modules updates are installed.
- KLRAMDISK is not supported on protected devices running the Windows XP or Windows Server® 2003 operating system.
- If Kaspersky Industrial CyberSecurity for Nodes patch installation fails, the patch is rolled back and you are prompted to restart the operating system.

Interface

- In the Application Console, filtering in the Quarantine, Backup, System audit log or Task log is case sensitive.
- When configuring a protection or scan scope in the Application Console, you can use only one mask and only at the end of the path. Following are the examples of correct masks: `C:\Temp\Temp*`, `C:\Temp\Temp???.doc`, `C:\Temp\Temp*.doc`. This limitation does not affect configuration of the Trusted Zone.
- In the Application Console, in the **Telemetry collection servers** section, the time when the tasks are scheduled to run is not displayed. The **Start time** column is empty.
- Pop-up notifications for interface text elements longer than 256 characters are not displayed in the Kaspersky Security Center Administration Console or the Application Console.
- In the Kaspersky Security Center Administration Console, the **Select a user or a group of users** window displays only the first 50,000 users from the list of Kaspersky Security Center users. See Kaspersky Security Center Help for more details.

Security

- If the operating system's User Account Control feature is enabled, a user account must be part of the KICS Administrators group to be able to open the Application Console by double-clicking the application icon in the tray notification area. Otherwise, it will be necessary to login as a user who is allowed to open the Compact Diagnostic Interface or Microsoft Management Console snap-in.
- If User Account Control is enabled, you cannot uninstall the application via the Microsoft Windows Programs and Features window.

Exploit Prevention

- Exploit Prevention is unavailable if the apphelp.dll libraries are not loaded in the current environment configuration.
- Exploit Prevention is incompatible with the EMET utility from Microsoft on protected devices running the Microsoft Windows 10 operating system. Kaspersky Industrial CyberSecurity for Nodes blocks EMET if the Exploit Prevention component is installed on a protected device with the EMET utility installed.
- Exploit Prevention is incompatible with the SQL Server® 2012 Database Engine. If you install Kaspersky Industrial CyberSecurity for Nodes on the computer with installed MS SQL Server 2012, you must add the sqlos.dll library of the database server to the list of exclusions in the Exploit Prevention task.

Detection and Response

- If in the course of the threat response process, a shared folder access error occurs, such an error is not reflected in the threat response history (Kaspersky Security Center Web Console → properties of the host with the installed application → **Detection and Response** – **Response history** section).

- Viewing the threat response history is not available for protected devices running Windows XP with Network Agent version 10.5.1781 installed.

- Kaspersky Industrial CyberSecurity for Nodes version 4.5 does not support the following EDR Expert (on-premises) telemetry events:

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  Starting with version 5.0, Kaspersky Industrial CyberSecurity for Nodes supports all of these EDR Expert (on-premises) telemetry events except LDAP Attribute Change.

- Migrating the [KICS+KEA] configuration to [KICS+built-in agent] configuration may complete with a Kaspersky Endpoint Agent application removal error. The application removal error is fixed in the latest version of Kaspersky Endpoint Agent. To remove Kaspersky Endpoint Agent, restart the computer and create an application removal task.

- The [KICS+KEA+built-in agent] configuration is not supported. Such configuration disrupts the interaction between applications and the Detection and Response solution that is deployed in your organization. In addition, using Kaspersky Endpoint Agent and the built-in agent on the same computer can lead to duplication of telemetry and increased load on the computer and network. After migrating to [KICS + built-in agent] configuration, make sure that Kaspersky Endpoint Agent has been removed from the computer. If Kaspersky Endpoint Agent continues to work after migration, uninstall the application manually (for example, using the *Uninstall application remotely* task).

  The installer allows you to deploy Kaspersky Endpoint Agent on a computer with Kaspersky Industrial CyberSecurity for Nodes and the built-in agent installed. Kaspersky Endpoint Agent and the built-in agent can also be installed on one computer as a result of the *Change application components* task. The behavior depends on the versions of Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent.

Event configuration

Settings of the *Uncontrolled file operation in controlled area* event that can be configured in the **Event configuration** section of the Kaspersky Security Center policy are also applied to the following events:

- *Allowed file operation in a controlled area performed by a trusted user*.
- *Prohibited file operation in controlled area*.
- *Statistics only: prohibited file operation in controlled area*.
- *Uncontrolled file operation in controlled area*.

Compact Diagnostic Interface

On Windows XP computers, Compact Diagnostic Interface requires the Terminal Service to be working.

Device Control

When uninstalling and reinstalling the application without a restart, Device Control may stay enabled. To restore the correct operation of Device Control, restart the computer.

Working in Windows Safe Mode

The application cannot work in Windows Safe Mode.

Typical deployments

Kaspersky Industrial CyberSecurity for Nodes is a part of Kaspersky Industrial CyberSecurity solution.

Kaspersky Industrial CyberSecurity solution includes the following utility and applications:

- Kaspersky Security Gateway.
- Kaspersky Industrial CyberSecurity for Nodes.
- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes work at different levels of a *dedicated network*. A dedicated Kaspersky Industrial CyberSecurity network is part of an industrial network that includes computers designed to run Kaspersky Industrial CyberSecurity applications to protect industrial systems and auxiliary hardware (for example, switches).

Kaspersky Industrial CyberSecurity for Networks monitors and analyzes industrial network traffic. Kaspersky Industrial CyberSecurity for Nodes, which is installed on an industrial network node, protects the computer from known computer security threats and monitors the integrity of PLC projects included in the scan scope.

You can control Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes deployed on the same dedicated network using a single Kaspersky Security Center Administration Console. You can also configure the diagnostic information received from Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes to be sent from Kaspersky Security Center to the SCADA system using Kaspersky Security Gateway.

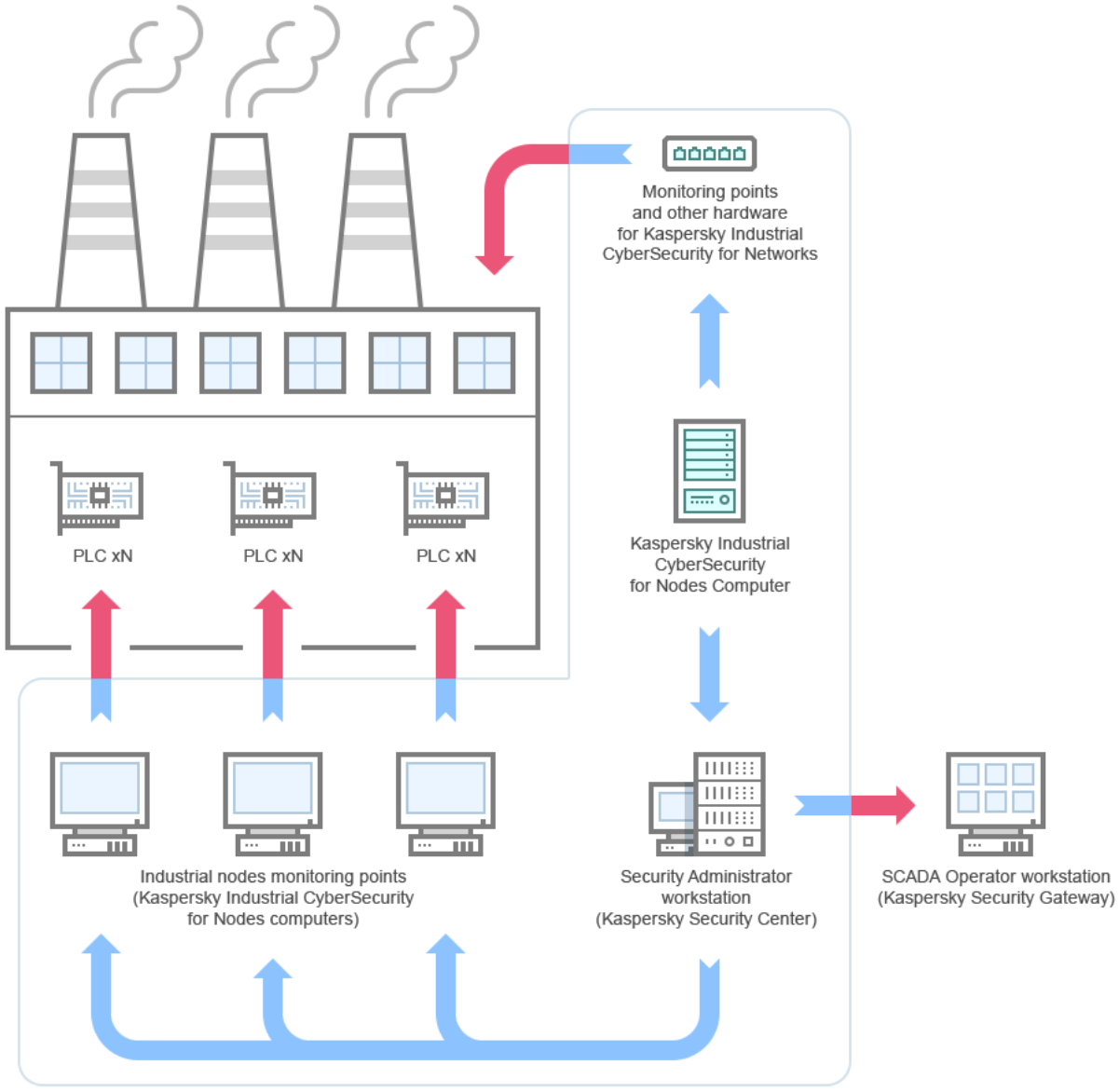
Kaspersky Industrial CyberSecurity for Nodes includes:

- *Functional module* – records information about the state of industrial network nodes and protects nodes from data threats.

- *Console* – is the local graphical user interface. You can use the Kaspersky Industrial CyberSecurity for Nodes Console to control the application on industrial network nodes. The Console may be installed on a computer with Kaspersky Industrial CyberSecurity for Nodes installed or any other computer on the protected network. In this case, the Console is used to control the application remotely. You can also use one Console to control several computers protected by Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes records security events on the protected nodes and sends the events to the Application Console and the Kaspersky Security Center Administration Console. The local Application Console and the Kaspersky Security Center Administration Console are accessed from the workstation of the specialist monitoring the industrial process at the enterprise, and from the workstation of the information security specialist.

In the example of the deployment of Kaspersky Industrial CyberSecurity for Nodes as part of the Kaspersky Industrial CyberSecurity solution (see the figure below), the dedicated network is shown in blue and the industrial network components are shown in red. The deployment scheme depends on the particulars of the industrial network in which the applications of the Kaspersky Industrial CyberSecurity solution are planned to be installed.



Kaspersky Industrial CyberSecurity for Nodes deployment scheme

Compatibility with other applications

Kaspersky Industrial CyberSecurity for Nodes in *Full functionality* configuration is incompatible with applications that are part of third-party endpoint protection systems (Endpoint Protection Platform, EPP). Kaspersky Industrial CyberSecurity for Nodes may also be incompatible with other applications and some Kaspersky applications. To determine compatibility, Kaspersky Industrial CyberSecurity for Nodes consults a list of software prepared by Kaspersky. This list is contained in the incompatible.txt file. This file is included in the distribution kit.

If an application from the incompatible.txt list is detected, the installer aborts the installation of Kaspersky Industrial CyberSecurity for Nodes. You need to remove the third-party anti-virus application. The installer may automatically delete some applications from the list.

If the Windows Firewall is installed on the computer, the installer turns it off to proceed with the installation of Kaspersky Industrial CyberSecurity for Nodes.

If, despite the risks, you need to install Kaspersky Industrial CyberSecurity for Nodes alongside an application from the incompatible.txt list on the same device, you can skip the check for installed third-party anti-virus applications. To do so, when running the installer, specify the following parameters: `SKIPPRODUCTCHECK=1` and `SKIPPRODUCTUNINSTALL=1`.

Example:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

Kaspersky Industrial CyberSecurity for Nodes in the *Endpoint Agent* configuration can be installed on the same computer as third-party EPP applications.

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Industrial CyberSecurity for Nodes.

Installation planning

This section describes the set of Kaspersky Industrial CyberSecurity for Nodes administration tools, and special aspects of installing and uninstalling Kaspersky Industrial CyberSecurity for Nodes using a wizard, command line, using Kaspersky Security Center and via an Active Directory group policy.

If you are installing Kaspersky Industrial CyberSecurity for Nodes after removing Kaspersky Embedded Systems Security for Windows or Kaspersky Endpoint Security for Windows, you must restart the computer.

Before starting installation of Kaspersky Industrial CyberSecurity for Nodes, plan the main stages of the installation.

1. Determine which administration tools will be used to manage and configure Kaspersky Industrial CyberSecurity for Nodes.
2. Select the necessary application components for installation.
3. Select the installation method.

Selecting administration tools

Determine the administration tools that will be used to configure Kaspersky Industrial CyberSecurity for Nodes settings and to manage the application. Kaspersky Industrial CyberSecurity for Nodes can be managed using the Application Console, command-line utility, and Kaspersky Security Center Administration Console.

Kaspersky Industrial CyberSecurity for Nodes Console

Kaspersky Industrial CyberSecurity for Nodes Console is a standalone snap-in added to the Microsoft Management Console. Kaspersky Industrial CyberSecurity for Nodes can be managed via the Application Console installed on the protected device or on another device on the corporate network.

Multiple Kaspersky Industrial CyberSecurity for Nodes snap-ins can be added to one Microsoft Management Console opened in author mode to use it to manage the protection of multiple device with Kaspersky Industrial CyberSecurity for Nodes installed.

Command line utility

You can manage Kaspersky Industrial CyberSecurity for Nodes from the command line of a protected device.

The command line utility is included in the Kaspersky Industrial CyberSecurity for Nodes software components group.

Kaspersky Security Center

If Kaspersky Security Center is used for centralized management of anti-virus protection of devices at your company, you can manage Kaspersky Industrial CyberSecurity for Nodes via the Kaspersky Security Center Administration Console.

The following components must be installed:

- **Module for integration with Kaspersky Security Center Network Agent**. This component is included in the Kaspersky Industrial CyberSecurity for Nodes software components group. It allows Kaspersky Industrial CyberSecurity for Nodes to communicate with the Network Agent. Install the module for integration with Kaspersky Security Center Network Agent on the protected device.

- **Kaspersky Security Center Network Agent**. Install this component on each protected device. This component supports interaction between Kaspersky Industrial CyberSecurity for Nodes installed on the protected device and Kaspersky Security Center Administration Console. The Network Agent installation file is included in the Kaspersky Security Center distribution kit folder.

- **Kaspersky Industrial CyberSecurity for Nodes Management Plug-in**. Additionally, install the Administration Plug-in for managing Kaspersky Industrial CyberSecurity for Nodes via the Administration Console on the protected device where the Kaspersky Security Center Administration Server is installed. This provides the interface for application management via Kaspersky Security Center. The Administration Plug-in installation file, \exec\klcfginst.exe, is included in the Kaspersky Industrial CyberSecurity for Nodes distribution kit.

Selecting the installation type

After specifying the software components for installation of Kaspersky Industrial CyberSecurity for Nodes, you need to select the application installation method.

Select the installation method depending on the network architecture and the following conditions:

- Whether you need special Kaspersky Industrial CyberSecurity for Nodes installation settings, or the recommended installation settings.

- Whether the installation settings will be the same for all protected devices or specific to each protected device.

Kaspersky Industrial CyberSecurity for Nodes can be installed interactively using the Setup Wizard or in silent mode without user involvement, and can be invoked by running the installation package file with installation settings from the command line. A centralized remote installation of Kaspersky Industrial CyberSecurity for Nodes can be performed using Active Directory group policies or using the Kaspersky Security Center remote installation task.

Kaspersky Industrial CyberSecurity for Nodes can be installed and configured on a single protected device with its settings saved to a configuration file; the file can then be used to install Kaspersky Industrial CyberSecurity for Nodes on other protected devices. Note that this ability does not exist when the application is installed using Active Directory group policies.

Starting the Setup Wizard

The Setup Wizard can install the following:

- Kaspersky Industrial CyberSecurity for Nodes components on the protected device, by clicking the link in the welcome application, which can be started by opening setupui.exe or directly using \exec\setup_kics.exe file in the distribution kit.

- Kaspersky Industrial CyberSecurity for Nodes Console on the protected device or other device on the LAN, by clicking the link in the welcome application, which can be started by opening setupui.exe or directly using \client\setup_kicstools.exe file in the distribution kit.

Running the installation package file from the command line with the necessary installation settings

If the installation package file is started without command-line options, Kaspersky Industrial CyberSecurity for Nodes will be installed with the default settings. Kaspersky Industrial CyberSecurity for Nodes options can be used to modify the installation settings.

The Application Console can be installed on the protected device and / or administrator's workstation.

You can also use sample commands for the installation of Kaspersky Industrial CyberSecurity for Nodes and the Application Console.

Centralized installation via Kaspersky Security Center

If Kaspersky Security Center is used in your network for managing networked devices' anti-virus protection, Kaspersky Industrial CyberSecurity for Nodes can be installed on multiple devices by using the remote installation task.

The protected devices on which you want to install Kaspersky Industrial CyberSecurity for Nodes using Kaspersky Security Center may be in the same domain as Kaspersky Security Center in a different domain, or in no domain at all.

Centralized installation using Active Directory group policies

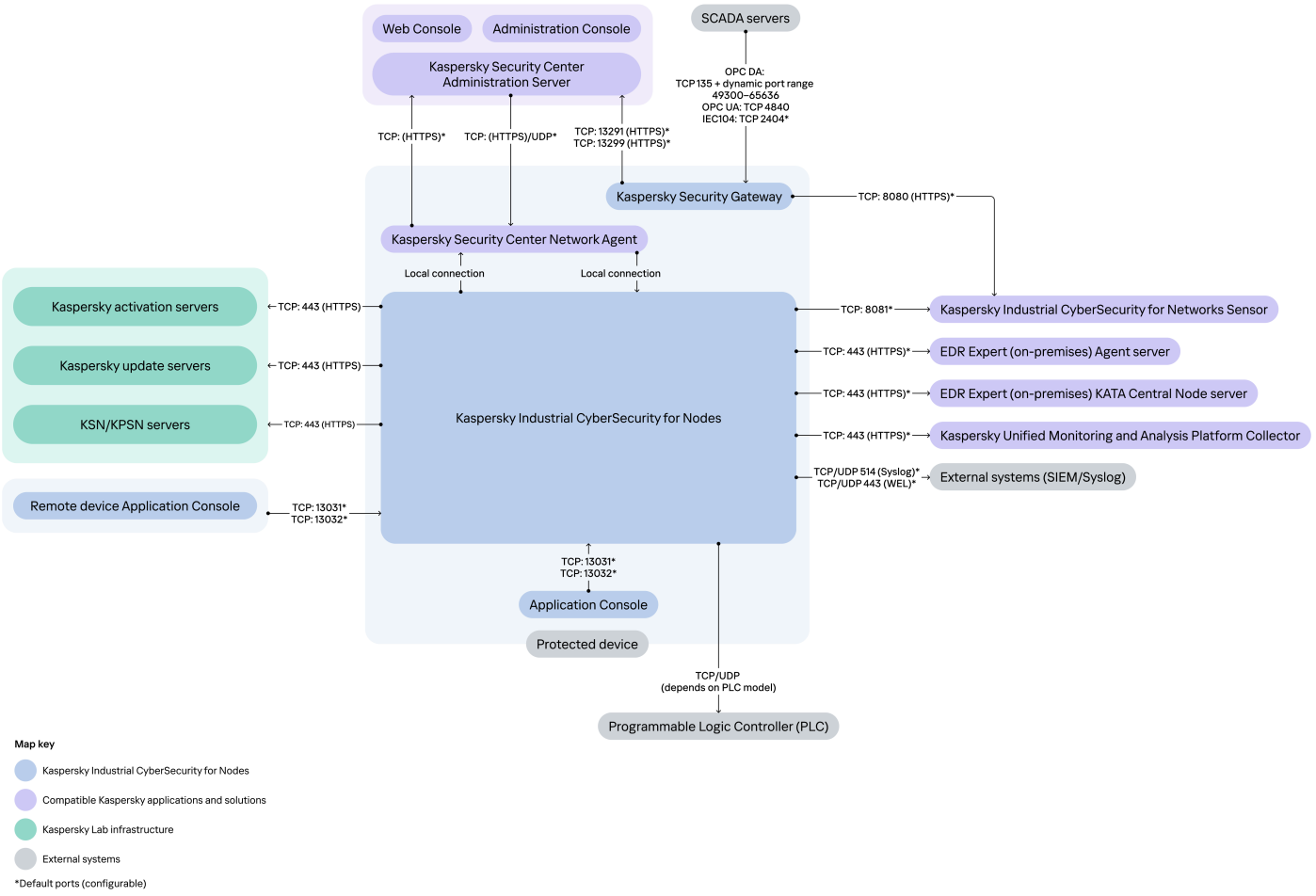
Active Directory group policies can be used to install Kaspersky Industrial CyberSecurity for Nodes on the protected device. The Application Console can be installed on the protected device or administrator's workstation.

Kaspersky Industrial CyberSecurity for Nodes can be installed using just the recommended installation settings.

The protected devices on which Kaspersky Industrial CyberSecurity for Nodes is installed using Active Directory group policies must be located in the same domain and the same organizational unit. Installation is performed at protected device start before logging in to Microsoft Windows.

Ports used

To install and run the components of Kaspersky Industrial CyberSecurity for Nodes, the ports indicated in the diagram below must be opened in the settings of the network equipment or the network traffic control software.



Ports used by Kaspersky Industrial CyberSecurity for Nodes

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

Purpose of used ports

Purpose	Communicating parties		Default port	Custom port possible	Protocol
	Source	Destination			
Managing Kaspersky Industrial CyberSecurity for Nodes from Kaspersky Security Center	Kaspersky Security Center Administration Server	Kaspersky Security Center Network Agent	See the Kaspersky Security Center Help	Yes	TCP (HTTPS), UDP (see the Kaspersky Security Center Help)
	Kaspersky Security Center Network Agent	Kaspersky Security Center Administration Server			

Purpose	Communicating parties		Default port	Custom port possible	Protocol
	Source	Destination			
Managing the application using the Kaspersky Industrial CyberSecurity for Nodes Console	Application Console	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	Yes	TCP
	Application console on the remote device	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	Yes	TCP
Kaspersky Industrial CyberSecurity for Nodes database and software modules update	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky update servers	443	No	TCP (HTTPS)
Activation of Kaspersky Industrial CyberSecurity for Nodes	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky activation servers	443	No	TCP (HTTPS)
KSN Usage	Kaspersky Industrial CyberSecurity for Nodes	KSN / KPSN servers	443	No	TCP (HTTPS)
Kaspersky Industrial CyberSecurity for Networks Integration	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky Industrial CyberSecurity for Networks sensor	8081	Yes	TCP
Using Kaspersky Security Gateway	Kaspersky Security Gateway	Kaspersky Security Center Administration Server	13291, 13299	Yes	TCP (HTTPS)
	Kaspersky Security Gateway	Kaspersky Industrial CyberSecurity for Networks sensor	8080	Yes	TCP (HTTPS)
	SCADA servers	Kaspersky Security Gateway	OPC DA: 135 + dynamic port range 49300–65635 OPC UA: 4840 IEC104: 2404	Yes	TCP
Endpoint Detection and Response Expert (on-premises) Integration	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert (on-premises) Agent server	443	Yes	TCP (HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert (on-premises) KATA Central Node server	443	Yes	TCP (HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	KUMA collector	443	Yes	TCP (HTTPS)

Purpose	Communicating parties		Default port	Custom port possible	Protocol
	Source	Destination			
Industrial Network Protection	Kaspersky Industrial CyberSecurity for Nodes	Siemens SIMATIC S7-300	102	Yes	TCP
		Siemens SIMATIC S7-400			
		Siemens SIMATIC S7-400H			
		Siemens SIMATIC S7-1200			
		Siemens SIMATIC S7-1500			
		Siemens SIPROTEC 4	50000	Yes	UDP
		Schneider Electric Modicon M340	502	Yes	TCP
		Schneider Electric Modicon M580			
		Devices based on CODESYS V3	11740	Yes	TCP
		OWEN PLC210			
		Fastwel CPM723-01			
		Prosoft Systems Regul R500			
		Emerson DeltaV	23 (Telnet), 18550	Yes	TCP
		Rockwell Automation Allen-Bradley ControlLogix	44818	Yes	TCP
		TREI-5B	6000	Yes	TCP
SIEM Integration	Kaspersky Industrial CyberSecurity for Nodes	SIEM / Syslog server	Syslog: 514 WEL: 443	Yes	TCP/UDP (customizable)

Installing and uninstalling the application using a wizard

This section describes the installation and uninstallation of Kaspersky Industrial CyberSecurity for Nodes and the Application Console by means of the Setup Wizard, and contains information about additional configuration of Kaspersky Industrial CyberSecurity for Nodes and actions to be performed upon installation.

Installing using the Setup Wizard

The following sections contain information about installation of Kaspersky Industrial CyberSecurity for Nodes and the Application Console.

To install and proceed to use Kaspersky Industrial CyberSecurity for Nodes:

1. Install Kaspersky Industrial CyberSecurity for Nodes on a protected device.
2. Install the Application Console on the devices from which you intend to manage Kaspersky Industrial CyberSecurity for Nodes.
3. If the Application Console has been installed on any device in the network other than the protected device, perform additional configuration to allow Application Console users to manage Kaspersky Industrial CyberSecurity for Nodes remotely.
4. Perform actions after installation of Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes installation

Before installing Kaspersky Industrial CyberSecurity for Nodes, do the following:

1. Make sure no other anti-virus applications are installed on the protected device.
2. Make sure that the account you use to run the Setup Wizard belongs to the administrators group on the protected device.

After completing the actions described above, proceed with the installation procedure. Following the Setup Wizard instructions, specify the installation settings for Kaspersky Industrial CyberSecurity for Nodes.

You can read more about the installation (uninstallation) settings.

To install Kaspersky Industrial CyberSecurity for Nodes via the Installation Wizard:

1. Run the setupui.exe file on the protected device.
2. In the window that opens, under **Installation**, follow the **Install Kaspersky Industrial CyberSecurity for Nodes 5.0** link.
3. In the welcome screen of the Kaspersky Industrial CyberSecurity for Nodes Setup Wizard, click the **Next >** button.

   The **End User License Agreement** window opens.
4. Review the terms of the License Agreement and Privacy Policy.
5. If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select the **I confirm that I have fully read, understand, and accept the terms and conditions of these End User License Agreements** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes.

   > If you do not accept the End User License Agreement and/or Privacy Policy the installation will be aborted.
6. Click **Next >**.

The **Custom installation** window opens. Select the components to be installed.

- **Full functionality**

  By default, all Kaspersky Industrial CyberSecurity for Nodes components other than Performance Counters and Endpoint Agent, are among those recommended for installation.

  The SNMP Protocol Support component of Kaspersky Industrial CyberSecurity for Nodes will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the protected device.

- **Endpoint Agent**

  When you select this option, Kaspersky Industrial CyberSecurity for Nodes is installed in the Endpoint Agent configuration. For detailed information about this configuration, see this section.

7. Click **Next >**.

8. In the **Select destination folder** window, do the following:

   - If required, specify a folder to which Kaspersky Industrial CyberSecurity for Nodes files will be copied.

   - If required, review the information about available space on local drives by clicking the **Browse** button.

9. Click **Next >**.

10. In the **Change default folders** window, you can edit the path to folders that the application uses.

    Application installation finishes with an error if the path to the installation folder is the same as the path to at least one of the following folders: application database folder, Backup folder, folder for restoring objects from Quarantine, temporary file folder.

11. In the **Advanced settings** window, you can exclude objects and folders from the protection scope and configure Real-Time File Protection.

    If required, select an industrial application exclusion profile: an XML set of configuration rules for adding industrial application processes and files to lists of trusted processes and exclusions, and for configuring Applications Launch Control rules and settings.

    If the Real-Time File Protection run mode is not selected, you cannot proceed to the next step of the Setup Wizard.

12. Click **Next >**.

13. In the **Import settings from configuration file** window, specify a path to the configuration file, if you want to import Kaspersky Industrial CyberSecurity for Nodes settings from an existing configuration file created in a previous version of the application.

14. Click **Next >**.

15. In the **Remote access settings** section, if necessary, change the TCP port numbers that the Application Console uses for the remote connection to the computer with the application installed.

    The default port number for connection with Windows credentials is 13032, and the default port number for connection with credentials of manually created users is 13031. Range of possible port numbers: 1–65535.

To prevent connection with credentials of manually created user accounts, clear the **Using credentials from manually created users** check box.

16. Click **Next >**.

17. In the **Activation of the application** window, do one of the following:

    - If you want to activate the application, specify a Kaspersky Industrial CyberSecurity for Nodes key file for application activation.
    - If you want to activate the application later, click the **Next >** button.
    - If a key file was previously saved in the \exec folder of the distribution kit, the name of this file will be displayed in the **Key** field.

    Once the key file is added, license information will be shown in the window. Kaspersky Industrial CyberSecurity for Nodes displays the license's calculated expiration date. The license term runs from the time when you add a key and expires no later than the expiration date of the key file.

18. Click **Next >** to add the key file to the application.

19. In the **Ready to install** window, you can disable the **Protect the installation process** option if necessary. Installation protection includes protection against replacement of the distribution package with malicious applications, blocking access to the installation folder of Kaspersky Industrial CyberSecurity for Nodes, and blocking access to the system registry section containing application keys. However, if the application cannot be installed (for example, when performing remote installation with the help of Windows Remote Desktop), you are advised to disable protection of the installation process.

20. If necessary, add the kavshell.exe file path to the %PATH% system variable for convenient use of the command line interface.

21. Click **Install**.

    The wizard will start installing Kaspersky Industrial CyberSecurity for Nodes. The **Finished the application Setup Wizard** window opens when installation is complete.

22. Click the **Finish** button.

Kaspersky Industrial CyberSecurity for Nodes Console installation

Follow the instructions of the Setup Wizard to configure installation settings for the Application Console. The installation process can be stopped at any step of the wizard. To do so, click the **Cancel** button in the Setup Wizard window.

To install the Kaspersky Industrial CyberSecurity for Nodes Console, run:

1. Make sure that the account you use to run the Setup Wizard belongs to the administrators group on the device.

2. Run the setupui.exe file on the protected device.

   The welcome window opens.

3. Click the **Install Kaspersky Industrial CyberSecurity for Nodes Console** link.

   The Setup Wizard's welcome window opens.

4. Click **Next >**.

5. If you agree to the terms and conditions of End User License Agreements and Privacy Policy, select the **I confirm that I have fully read, understand, and accept the terms and conditions of these End User License Agreements** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes.

6. If required, specify a different folder to which the files being installed should be saved in the **Select destination folder** window.

7. Click **Next >**.

8. Click the **Install** button in the **Ready to install** window.

   The wizard will start installing the Kaspersky Industrial CyberSecurity for Nodes Console.

9. Click **Finish**.

The Application Console will be installed.

If the Application Console has been installed on any device in the network other than the protected device, configure the advanced settings.

Advanced settings after installation of the Application Console on another device

If the Application Console has been installed on any device in the network, other than a protected device, perform the following actions to allow users to manage Kaspersky Industrial CyberSecurity for Nodes remotely:

- Use a user account that has permission to connect remotely in the application settings. By default, all users in the Administrators and KICS Administrators groups have this permission.

- On the remote device, in the Windows Firewall settings, open the TCP 13032 port for connection by Windows system user accounts and TCP 13031 for connection by user accounts manually created in application settings. Also allow network connections for the executable file of the Kaspersky Industrial CyberSecurity for Nodes remote management process, avp.exe. You can manage this setting using the `ADDWFEXCLUSION=1` option when installing the application on the command line.

If you need to run Kaspersky Industrial CyberSecurity for Nodes remotely, additionally do the following:

The user account that will remotely start the application must be part of the Administrators group. Make sure that this account has necessary permissions to manage Kaspersky Industrial CyberSecurity for Nodes as well as to manage the Kaspersky Industrial CyberSecurity for Nodes Service.

- On the remote device, in the Windows Firewall settings, enable the **File and Printer Sharing (SMB-In)** rule (port TCP 445). We also recommend opening port TCP 135 to facilitate the connection to the device.
- For remote devices running Windows Vista or later that are not part of a domain or are managed by a local user account, **disable remote control of user accounts (UAC).**

  1. Open the registry editor on the computer.
  2. In the registry editor, open the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System key.
  3. Open the LocalAccountTokenFilterPolicy value.

     If the LocalAccountTokenFilterPolicy value is missing under this key, create a DWORD (32-bit) value with this name (for details, refer to the Microsoft Technical Support website).
  4. Set it to `1` and click **OK**.

     Disabling remote UAC does not affect local UAC.
- If the device on which the Application Console is installed or the protected device run Windows 8.1 or an earlier version of Windows, **enable the support of shared access to SMB 1.0/CIFS files on devices running Windows 10 or later.**

  - In the "Windows Features" application:

    1. Select **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
    2. In the **Windows Features** window, select the **SMB 1.0/CIFS File Sharing Support** check box.
    3. Click **OK**.
  - In Windows PowerShell:

    1. Run Windows PowerShell as administrator.
    2. Run the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

The same steps should be applied to configure any other software or hardware firewall.

If the Application Console is open while you configure the connection between the protected device and the device on which the Application Console is installed:

1. Close the Application Console.
2. Wait until the Kaspersky Industrial CyberSecurity for Nodes remote management process avp.exe is finished.
3. Restart the Application Console.

   The new connection settings will be applied.

Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation

Kaspersky Industrial CyberSecurity for Nodes starts protection and scan tasks immediately after installation if you have activated the application. If **Enable Real-Time File Protection after installation of application (recommended)** (default option) is selected during installation of Kaspersky Industrial CyberSecurity for Nodes, the application scans the device's file system objects when they are accessed. If the Script monitoring component was installed as part of custom installation, Kaspersky Industrial CyberSecurity for Nodes scans the source code of all scripts when they are started. Kaspersky Industrial CyberSecurity for Nodes will run the *Critical Areas Scan* task every Friday at 8:00 P.M.

We recommend that you take the following steps after installing Kaspersky Industrial CyberSecurity for Nodes:

- Start the application database update task. After installation Kaspersky Industrial CyberSecurity for Nodes will scan objects using the database included in the application distribution kit.

  > We recommend updating Kaspersky Industrial CyberSecurity for Nodes databases immediately since they may be out of date.

  The application will then update the databases every hour according to the default schedule configured in the task.

- Run a Critical Areas Scan of the device if no anti-virus software with real-time file protection was installed on the device before installation of Kaspersky Industrial CyberSecurity for Nodes.
- Configure administrator notifications about Kaspersky Industrial CyberSecurity for Nodes events.

Starting and configuring the Update of databases and application modules task

To update the application database after installation:

1. Under *Update*, configure the connection to the update source.
2. Run the *Update* task.

Web Proxy Auto-Discovery Protocol (WPAD) may not be configured on your network to detect proxy server settings automatically in the LAN. At that, your network may require authentication when accessing the proxy server.

To specify the optional proxy server settings and authentication settings for accessing the proxy server:

1. In the Application Console, open the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.
2. Select **Application properties**.
3. This opens a window; in that window, select the **Network settings** tab.
4. In the **Proxy server settings** section, click **Settings** and in the displayed window, select the **Use specified proxy server settings** check box.
5. Enter the proxy server address in the **Address** field, and enter the port number for the proxy server in the **Port** field.
6. If necessary, clear the **Bypass a proxy server for local addresses** check box. If this functionality is enabled, devices are accessed directly from the network that hosts the protected device with Kaspersky Industrial CyberSecurity for Nodes installed. This option is enabled by default.
7. In the **Proxy server authentication settings** section, select the necessary authentication method in the drop-down list:
   - **Do not use authentication**.
   - **NTLM authentication**. NTLM authentication with the current user account (default).
   - **NTLM authentication with user name and password**. NTLM authentication with manually specified credentials.
   - **Kerberos authentication**. Kerberos authentication with the current user account.

     To ensure the Kerberos authentication works correctly when using CNAME records for the proxy server address, you must register a Service Principal Name (SPN) for each CNAME record.

   - **Kerberos authentication with user name and password**. Kerberos authentication with manually specified credentials.
   - **User name and password**. Authentication with manually specified credentials.

   Enter the user name and password, if needed.

   If Kerberos authentication is selected, Kaspersky Industrial CyberSecurity for Nodes can, depending on the proxy server settings, perform authentication using either the Kerberos or NTLM protocol.
8. Click **OK**.

To run the Update task:

1. In the Application Console tree, expand the **Update** node.
2. In the context menu of the **Database update** child node, select the **Start** item.

The *Update* task is started.

After the task has successfully completed, you can view the release date of the latest database updates installed in the results pane of the **Kaspersky Industrial CyberSecurity for Nodes** node.

Critical Areas Scan

After you have updated the Kaspersky Industrial CyberSecurity for Nodes databases, scan the protected device for malware using the *Critical Areas Scan* task.

To run the Critical Areas Scan task:

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. In the context menu of the **Critical Areas Scan** child node, select the **Start** command.

The task starts; the **Running** task status is displayed in the results pane.

To view the task log,

in the results pane of the **Critical Areas Scan** node, click the **Open task log** link.

Modifying the set of components and repairing Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes components can be added or removed. You need to stop the Real-Time File Protection task before removing the Real-Time File Protection component. In other circumstances there is no need to stop the Real-Time File Protection task or the Kaspersky Industrial CyberSecurity for Nodes Service.

If application management is password protected, Kaspersky Industrial CyberSecurity for Nodes requests the password when you attempt to remove components or modify the set of components in the Setup Wizard.

To modify the set of Kaspersky Industrial CyberSecurity for Nodes components:

1. In the Windows **Control Panel**, select **Apps & features**. The **Modify or Remove** window opens.
2. Right-click **Kaspersky Industrial CyberSecurity for Nodes** and select **Edit**.

   This opens the Setup Wizard **Modify, repair, or remove application**.
3. Select **Modify**.

   The **Custom installation** window opens. Select **Full functionality** and click **Next >**.

4. In the **Custom installation** window, in the list of available components, select the components that you want to add or remove from Kaspersky Industrial CyberSecurity for Nodes. To do this, perform the following actions:

   - To change the set of components, click the button next to the name of the selected component. Then in the context menu, select:

     - **Feature will be installed on the local hard drive**, if you want to install one component;

     - **Entire feature and its subfeatures will be installed on local hard drive**, if you want to install the group of components;

   - To remove previously installed components, click the button next to the name of the selected component. In the context menu, select **Feature will be unavailable**.

   Click **Next >**.

5. In the **Ready to install** window, confirm the selection of application components by clicking **Install**.

6. In the window that opens when installation is complete, click the **Finish** button.

   The set of Kaspersky Industrial CyberSecurity for Nodes components will be modified based on the specified settings.

If problems occur during the operation of Kaspersky Industrial CyberSecurity for Nodes (Kaspersky Industrial CyberSecurity for Nodes crashes; tasks crash or do not start), you can perform a repair for Kaspersky Industrial CyberSecurity for Nodes. You can perform a repair while saving the current Kaspersky Industrial CyberSecurity for Nodes settings, or you can select an option to reset all Kaspersky Industrial CyberSecurity for Nodes settings to their default values.

To repair Kaspersky Industrial CyberSecurity for Nodes after the application or a task crashes:

1. In the Windows **Control Panel**, select **Apps & features**. The **Modify or Remove** window opens.

2. Right-click **Kaspersky Industrial CyberSecurity for Nodes** and select **Edit**.

3. This opens the Setup Wizard **Modify, repair, or remove application**.

4. Select the **Repair** option.

   The **Repair Kaspersky Industrial CyberSecurity for Nodes** window opens. Click **Next >**.

5. Wait until the restore operation completes and in the window that opens click **Finish**.

   Kaspersky Industrial CyberSecurity for Nodes will be repaired using the specified settings.

Uninstalling using the Setup Wizard

This section contains instructions on removing Kaspersky Industrial CyberSecurity for Nodes and the Application Console from a protected device using the Setup / Uninstallation Wizard.

Kaspersky Industrial CyberSecurity for Nodes uninstallation

Dump and trace files are not deleted on uninstalling Kaspersky Industrial CyberSecurity for Nodes. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

The names of settings may vary depending on the installed Windows operating system.

Kaspersky Industrial CyberSecurity for Nodes can be uninstalled from the protected device using the Setup / Uninstallation Wizard.

After uninstalling Kaspersky Industrial CyberSecurity for Nodes from a protected device a restart may be required. The restart can be postponed.

Uninstallation, repair and installation of the application is not available via the Windows Control Panel.

Kaspersky Industrial CyberSecurity for Nodes prompts for the user's account credentials when the user attempts to remove or modify the set of components in the Setup Wizard. You need to enter the credentials of a user with sufficient rights. If an empty Windows password is set for the user account that performs the removal, disable the **Request password to confirm critical actions** functionality before starting the removal.

To uninstall Kaspersky Industrial CyberSecurity for Nodes:

1. In the Windows **Control Panel**, select **Apps & features**. The **Modify or Remove** window opens.
2. Right-click **Kaspersky Industrial CyberSecurity for Nodes** and select **Edit**.
3. This opens the Setup Wizard **Modify, repair, or remove application**.
4. Select **Remove**.

   The **Save objects** window opens.
5. If required, in the **Save objects** window, do the following:

   Under **Save objects**, specify which objects or settings you want to keep. By default, the check boxes are cleared.

   - Select the **Activation data** check box.
   - Select the **Backup files** check box.
   - Select the **Operational settings of the application** check box.

Under **Export objects**, specify which objects you want to export. By default, the check boxes are cleared.

- Select the **Export quarantine objects** check box to make Kaspersky Industrial CyberSecurity for Nodes export objects that have been quarantined. By default, the check box is cleared.
- Check the **Export Backup objects** check box to export objects from Kaspersky Industrial CyberSecurity for Nodes Backup. By default, the check box is cleared.
- Click the **Save** button and select the folder to which you want to export the objects. By default, the objects will be exported to %ProgramData%\Kaspersky Lab\KICS.5.0\QB.

  Click **Next**.

6. In the **Ready to uninstall** window, confirm the removal by clicking **Remove**.
7. In the window that opens when the uninstallation is complete, click the **Finish** button.

Kaspersky Industrial CyberSecurity for Nodes will be uninstalled from the protected device.

Kaspersky Industrial CyberSecurity for Nodes Console uninstallation

The names of settings may vary depending on the installed Windows operating system.

You can uninstall the Application Console from the protected device using the Setup / Uninstallation Wizard.

After uninstalling the Application Console, you do not need to restart the protected device.

To uninstall the Application Console:

1. In the Windows **Control Panel**, select **Apps & features**. The **Modify or Remove** window opens.
2. Right-click **Kaspersky Industrial CyberSecurity for Nodes Console** and select **Edit**.

   This opens the window of the **Modify, repair, or remove application** wizard.
3. Select **Remove**.

   The **Ready to uninstall** window opens. Click **Uninstall**.
4. In the window that opens when the uninstallation is complete, click the **OK** button.

Uninstallation is now complete, and the Setup Wizard closes.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Industrial CyberSecurity for Nodes from the command line and contains examples of commands to install and uninstall Kaspersky Industrial CyberSecurity for Nodes from the command line, and examples of commands to add and remove Kaspersky Industrial CyberSecurity for Nodes components from the command line.

About installing and uninstalling Kaspersky Industrial CyberSecurity for Nodes from command line

Dump and trace files are not deleted on uninstalling Kaspersky Industrial CyberSecurity for Nodes. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

You can install or uninstall Kaspersky Industrial CyberSecurity for Nodes and add or remove its components by running the \exec\kics_win.msi installation package file from the command line after you specify the installation settings using command-line options.

The Kaspersky Industrial CyberSecurity for Nodes Console can be installed on the protected device or on another device on the network to work with the application locally or remotely. To do this, use the \client\kicstools.msi installation package.

Perform the installation using an account included in the administrators group on the protected device where the application is installed.

If the \exec\kics_win.msi file is run on the protected device without additional command-line options, Kaspersky Industrial CyberSecurity for Nodes will be installed with the default installation settings.

You can assign the set of components to be installed using the ADDLOCAL command-line option and listing the codes for the selected components or sets of components.

Kaspersky Industrial CyberSecurity for Nodes software component codes for the Windows Installer service

The \exec\kics_win.msi file is designed to install Kaspersky Industrial CyberSecurity for Nodes.

The \client\kicstools.msi file is designed to install the Kaspersky Industrial CyberSecurity for Nodes Console.

The following table contains codes and descriptions of Kaspersky Industrial CyberSecurity for Nodes software components.

Description of Kaspersky Industrial CyberSecurity for Nodes software components

Component	Code	Component functions
Real-Time File Protection	`FileThreatProtection`	This component performs virus scans of files on the protected device when these files are accessed.
AMSI Scanner	`AMSI`	This component is intended to support Antimalware Scan Interface from Microsoft. The Antimalware Scan Interface (AMSI) allows third-party applications with AMSI support to send objects (for example, PowerShell scripts) to Kaspersky Industrial CyberSecurity for Nodes for an additional scan and then receive the results from scanning these objects.
Anti-Cryptor	`BehaviorDetection`	This component fills the list of blocked hosts with names of remote devices that show malicious activity.
Exploit Prevention	`ExploitPrevention`	This component makes it possible to manage settings to protect memory used by processes in a device's memory.

Component	Code	Component functions
Remediation Engine	`RemediationEngine`	This component allows Kaspersky Industrial CyberSecurity for Nodes to roll back actions that have been performed by malware in the operating system.
Firewall	`Firewall`	This component makes it possible to manage Windows Firewall through the Kaspersky Industrial CyberSecurity for Nodes graphical user interface.
Network Threat Protection	`NetworkThreatProtection`	This component scans inbound network traffic for activity that is typical of network attacks. Upon detecting an attempted network attack that targets your computer, Kaspersky Industrial CyberSecurity for Nodes blocks network activity from the attacking computer.
Applications Launch Control	`ApplicationControl`	This component monitors user attempts to start applications and allows or denies application launch in accordance with specified Applications Launch Control rules.
Device Control	`DeviceControl`	This component tracks attempts to connect external devices to a protected device and allows or denies use of these devices according to the specified device control rules.
Module for integration with Kaspersky Security Center Network Agent	`AdminKitConnector`	Provides a connection between the Kaspersky Industrial CyberSecurity for Nodes and the Kaspersky Security Center Network Agent. You can install this component on the protected device if you intend to manage the application via Kaspersky Security Center.
Log Inspection	`LogInspector`	This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.
System Integrity Monitoring	`SystemIntegrityMonitor`	This component includes all functionality of File Integrity Monitor and additionally allows monitoring registry changes and connection of external devices.
Endpoint Detection and Response (Industrial CyberSecurity)	`EDR`	This component facilitates interaction with the Kaspersky Industrial CyberSecurity Endpoint Detection solution.
Endpoint Detection and Response Expert (on-premises)	`AntiAPT`	This component facilitates integration with the Endpoint Detection and Response solution, which is part of Kaspersky Anti Targeted Attack Platform.
BadUSB Attack Prevention	`BadUSBAttackPrevention`	The component prevents infected USB devices emulating a keyboard from connecting to the computer.
Managed Detection and Response	`MDR`	This component facilitates interaction with the Kaspersky Managed Detection and Response solution.
Integration with KICS for Networks	`KicsForNetworks`	This component facilitates integration with Kaspersky Industrial CyberSecurity for Networks solution.
Portable Auditor	`PortableScanner`	This component allows you to scan isolated devices for viruses and other malware, record incoming and outgoing traffic of scanned devices for a specified time, and run a security audit on the devices.
PLC Project Investigation	`KicsPlcFeature`	This component allows receiving information about the PLC projects currently used in the industrial network.
PLC Project Integrity Check	`KicsPlcFeature`	This component allows checking the integrity of PLC projects used in an industrial system.
On-Demand Scan	`Ods`	This component installs Kaspersky Industrial CyberSecurity for Nodes system files and On-demand scan tasks (scanning of objects on the protected device upon request).
KSN Usage	`Ksn`	This component provides protection based on Kaspersky cloud technologies. The component implements sending requests to and receiving conclusions from the Kaspersky Security Network service.
Anomaly Detection using Sigma rules	`SigmaMonitoring`	This component uses Sigma rules to analyze the data of internal events and event logs for anomalies.
SIEM Integration	`SiemTelemetry`	This component lets you configure the integration with a SIEM server.

Installation and recovery settings, and Windows Installer command-line options

This section describes Kaspersky Industrial CyberSecurity for Nodes installation and recovery settings. The section also contains the keys for changing the installation settings and possible key values. These keys can be used in conjunction with standard keys for the Windows Installer service's `msiexec` command when installing Kaspersky Industrial CyberSecurity for Nodes from the command line.

Installation settings and Windows Installer command-line options

- Acceptance of the terms of the End User License Agreement.

  `EULA=<value>` can take the following values.

  - `0` – you reject the terms of the End User License Agreement (default value).
  - `1` – you accept the terms of the End User License Agreement.

- Acceptance of the terms of the Privacy Policy.

  `PRIVACYPOLICY=<value>` can take the following values.

  - `0` – you reject the terms of the Privacy Policy (default value).
  - `1` – you accept the terms of the Privacy Policy.

- Selecting the mode for the application.

  `STANDALONEMODE=<value>` can take the following values.

  - `0` – Full functionality (default value).
  - `1`: Endpoint Agent.

- Destination folder where Kaspersky Industrial CyberSecurity for Nodes files will be saved during installation. A different folder can be specified.

  The default value for the `INSTALLDIR=<full path to the folder>` command-line option is as follows:

  - For the 32-bit version of Microsoft Windows:
    - Kaspersky Industrial CyberSecurity for Nodes: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
    - Kaspersky Industrial CyberSecurity for Nodes Console: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0
  - For the 64-bit version of Microsoft Windows: %ProgramFiles(x86)% and further similarly to the paths for 32-bit versions of Microsoft Windows.

- Start of the *Real-Time File Protection* task immediately after Kaspersky Industrial CyberSecurity for Nodes starts.

  `RUNRTP=<value>` can take the following values.

  - `1` – start (default value).
  - `0` – do not start.

- The *Real-Time File Protection* task operating mode.

  `RTP_BLOCKING=<value>` can take the following values.

  - `1` – Recommended (default value).
  - `0` – Inform.

- Adding processes and files of industrial software to lists of trusted processes and exclusions as well as configuring Applications Launch Control rules. Processes and files are added to exclusions using the following command line option: `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`. Names of supported exclusion profiles are listed here.

- Path to the key file (`LICENSEKEYPATH`). By default, the Windows Installer attempts to find the file with .key extension in the \exec folder of the distribution kit. If the \exec folder contains several key files, the Windows Installer will select the key file whose expiration date is the farthest into the future. A key file can be saved beforehand in the \exec folder or at another path that you can specify in the `LICENSEKEYPATH` parameter.

  `LICENSEKEYPATH` can take the following values.

  - Full path to the key file including its name.
  - Path to the folder where the key files are stored.

  You can add a key after Kaspersky Industrial CyberSecurity for Nodes is installed using an administrative tool of your choice: for example, the Application Console. If you do not add a key during installation of the application, Kaspersky Industrial CyberSecurity for Nodes will not function.

- Path to the configuration file. Kaspersky Industrial CyberSecurity for Nodes imports settings from the specified configuration file created in the application. Kaspersky Industrial CyberSecurity for Nodes does not import passwords from the configuration file, for example, account passwords for starting tasks, or passwords for connecting to a proxy server. Once the settings are imported, you will have to enter all passwords manually. If the configuration file is not specified, the application will start to work with the default settings after setup.

  The default value for `CONFIGPATH=<configuration file name>` is not specified.

- *Scan at Operating System Startup* mode (`SCANSTARTUP_BLOCKING`). If Kaspersky Industrial CyberSecurity for Nodes was installed without a `SCANSTARTUP_BLOCKING` key, the **Scan scope** parameter in the *Scan at Operating System Startup* task is set as follows:

  - Action to perform on infected and other objects: **Inform**.
  - Action to perform on probably infected objects: **Inform**.

If Kaspersky Industrial CyberSecurity for Nodes was installed with a `SCANSTARTUP_BLOCKING` key, the **Scan scope** parameter in the *Scan at Operating System Startup* task is set as follows:

- Action to perform on infected and other objects: **Perform recommended action**.
- Action to perform on probably infected objects: **Perform recommended action**.

The *Scan at Operating System Startup* task is created automatically. The **Inform** mode is applied by default. In this case, after you deploy Kaspersky Industrial CyberSecurity for Nodes on the devices, you can enable the *Scan at Operating System Startup* task if no issues with system services were discovered during scan. If the application detects critical system services as infected or probably infected objects, the **Inform** mode gives you time to figure out the reason and solve the issue. If the application applies the **Perform recommended action** mode, the **Disinfect. Delete if disinfection fails** action is performed. Disinfection or removal of the system files may result in critical issues with operating system startup.

- Configuring the Protection of operating system services functionality.

  If this function is enabled, third-party applications cannot act upon the processes of the operating system. `PROTECTOSSERVICES=<value>` can take the following values.

  - `1` means that the protection of operating system services is enabled (default setting).
  - `0` means that the protection of operating system services is disabled.

- Configuring ports used for the remote connection of the Application Console to a computer on which the application is installed:

  To configure the port for connecting with Windows credentials, you can use the `UIPORT=<port number>` parameter. Range of possible port numbers: 1–65535. If the number is outside the specified interval, the default port number is used. The default value is 13032.

  If necessary, you can close the port for connecting with credentials of manually created users using the `ENABLEUIKLPORT=<value>` parameter:

  - `1` opens the port (default setting).
  - `0` closes the port.

  The default value for this port is 13031. You can change the port number by specifying the `UIKLPORT=<port>` parameter. Range of possible port numbers: 1–65535.

- Setting for enabling network connections for remote management of Kaspersky Industrial CyberSecurity for Nodes using the Application Console installed on a different computer.

  `ADDWFEXCLUSION=<value>` can take the following values.

  - `1` If this value is specified, TCP ports configured for the remote connection of the Application Console to a computer with the application installed (the `UIPORT=<port>` and `UIKLPORT=<port>` parameters) are opened in the Windows Firewall, and network connections are allowed for the executable file of the Kaspersky Industrial CyberSecurity for Nodes remote management process, avp.exe.

    Read also about additional configuration when installing the application on another device.

  - `0` If this value is specified, nothing happens.

- Disabling the check for incompatible software. Use this setting to enable or disable the check for incompatible software during background installation of the application on the protected device. Regardless of the value of this setting, during installation of Kaspersky Industrial CyberSecurity for Nodes, the application always warns about other versions of the application installed on the protected device.

The possible values for `SKIPPRODUCTCHECK=<value>` command line option are as follows (you can also use `SKIPINCOMPATIBLESW=<value>`):

- `0` – The check for incompatible software is performed (default value).
- `1` – The check for incompatible software is not performed.

- Disabling automatic removal of incompatible software.

  If the `SKIPPRODUCTUNINSTALL=1` option is specified, Kaspersky Industrial CyberSecurity for Nodes does not remove incompatible software. If this option is not specified, Kaspersky Industrial CyberSecurity for Nodes automatically attempts to remove incompatible software.

  > When installing Kaspersky Industrial CyberSecurity for Nodes using the msiexec installer, removal of incompatible software is not performed. To automatically remove the software that may cause compatibility issues, use setup_kics.exe file.

- Creating a unique computer identifier (Sensor ID) during the installation or update of the application.

  Sensor ID is used in the Kaspersky Anti Targeted Attack Platform solution to identify computers that send telemetry to the server. When creating Sensor ID, the application uses an algorithm that takes into account the computer's configuration, such as the motherboard serial number. In some cases, for example, when using the application in a virtual environment, Sensor ID may be duplicated. As a result, the Kaspersky Anti Targeted Attack Platform cannot identify the computer from which the telemetry is sent. To create a unique Sensor ID, you need to set the parameter `ENABLEUNIQUESENSORID=1`. As a result, the application will use a different algorithm to create the Sensor ID, which takes into account other data about the computer. This ensures that the Sensor ID is unique.

  By default, the parameter is not set. The application inherits the Sensor ID in the following cases:

  - updating the application version;
  - migrating the [KICS+KEA] configuration to [KICS+built-in agent] configuration.

  As part of application repair, the installer attempts to inherit the Sensor ID. If the Sensor ID cannot be restored, the application creates a new Sensor ID.

- Disabling the check for the KB5007186 operating system update.

  After installing the KB5007186 update, the application continues working normally, system security is not compromised, but minor version updates of the applications become impossible. Before installing the application, the installer checks for installed operating system updates. If update KB5007186 is discovered, the installer aborts the installation. You can use the `SKIPKB5007186CHECK` key on the command line to enable or disable the check for the KB5007186 operating system update.

  `SKIPKB5007186CHECK=<value>` can take the following values.

  - `0` – The installer checks if the KB5007186 operating system update is installed.
  - `1` – The installer does not check if the KB5007186 operating system update is installed.

  By default, the key is not set, which corresponds to `0`.

- Skip the installation of the DigiCert Assured ID Root CA root certificate to the trusted certificate store of the operating system.

  If the `SKIPINSTALLROOTCACERTIFICATES` option is specified when installing the application, the DigiCert Assured ID Root CA root certificate is not installed. By default, the certificate is automatically installed from the application installation package.

- Customizing blocking access to Rutoken removable drives. If blocking is enabled, on a device with the application, the user can only create a Portable Auditor and run *Secure copying of application databases* and *Secure update of application databases* tasks on the device; access to the protected removable drive using standard means of the operating system is blocked.

  `TOKENPROTECTION=<value>` can take the following values.

  - `0` – blocking is disabled (default value).
  - `1` – blocking is enabled.

Recovery settings and Windows Installer command-line options

- Restoring quarantined objects.

  `RESTOREQTN=<value>` can take the following values.

  - `0` – Remove quarantined content (default value).
  - `1` – Restore quarantined content to the folder specified by the `RESTOREPATH` parameter into the `\QB` subfolder.

- Restoring the content of backup.

  `RESTOREBCK=<value>` can take the following values.

  - `0` – Remove backup content (default value).
  - `1` – Restore backup contents to the folder specified by the `RESTOREPATH` parameter into the `\QB` subfolder.

- Enter the current password to confirm the restoration (if password protection is enabled).

  The default value for `UNLOCK_PASSWORD=<specified password>` is not specified.

- Folder for restored objects. Restored objects will be saved to the specified folder.

  The default value for the `RESTOREPATH=<full path to the folder>` command line option is `%ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KICS.5.0.0\QB\Restored`.

Example commands for installing Kaspersky Industrial CyberSecurity for Nodes

This section provides examples of commands used to install Kaspersky Industrial CyberSecurity for Nodes.

Run the kics_win.msi file from the distribution kit on the protected device.

Detailed information about the use of Windows Installer's standard commands and command-line options is provided in the documentation supplied by Microsoft.

Examples of installing Kaspersky Industrial CyberSecurity for Nodes from the setup_kics.exe file

To install Kaspersky Industrial CyberSecurity for Nodes with the recommended installation settings and without user involvement:

```
\exec\setup_kics.exe EULA=1 PRIVACYPOLICY=1
```

To install components, such as Device Control:

```
\exec\setup_kics.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

When installing Kaspersky Industrial CyberSecurity for Nodes on computers with network devices and SCSI devices that cause a system crash after installation, you can use the following additional options with this command:

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

Enables (1) or disables (0) interception of connections of network adapters.

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

Enables (1) or disables (0) interception of connections of SCSI adapters.

To install and activate Kaspersky Industrial CyberSecurity for Nodes using the key file:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

To change the port used for the remote connection of the Application Console to a computer on which the application is installed with Windows user credentials:

```
setup_kics.exe /pUIPORT=<port number>
```

Range of possible port numbers: 1–65535. The default value is 13032.

List of commands used for installation: running an .msi file

To install Kaspersky Industrial CyberSecurity for Nodes with the recommended installation settings and without user involvement:

```
msiexec /i kics_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Industrial CyberSecurity for Nodes with the recommended installation settings and display the installation interface:

```
msiexec /i kics_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Industrial CyberSecurity for Nodes with the recommended installation settings and enable trace file rotation when the number of trace files reaches the specified maximum number:

```
msiexec /i kics_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1 PRIVACYPOLICY=1
```

The `TRACE_FOLDER` parameter is required.

The following rules apply to the `TRACE_MAX_ROLL_COUNT` parameter:

- If this parameter is specified, trace file rotation is enabled when the number of trace files reaches the maximum number specified in the parameter. Available range of parameters values: from 1 to 999.
- If the maximum number of trace files is specified as 0, trace file rotation is disabled.
- If a parameter value is specified, but is invalid or outside the range of available values (from 1 to 999), trace file rotation is enabled with the default maximum number of trace files set to 5.
- If the parameter is not specified:
  - If trace file rotation is already configured on the device, its settings are not changed. The application will ignore the entered parameters.
  - If trace file rotation is not configured on the device, the rotation option will be enabled with the default maximum number of trace files set to 5.

To install and activate Kaspersky Industrial CyberSecurity for Nodes using the key file C:\0000000A.key:

```
msiexec /i kics_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Industrial CyberSecurity for Nodes with a preliminary scan of active processes and the boot sectors of local disks:

```
msiexec /i kics_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Industrial CyberSecurity for Nodes in the installation folder C:\KICS:

```
msiexec /i kics_win.msi INSTALLDIR=C:\KICS /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Industrial CyberSecurity for Nodes and save an installation log file named kics.log in the folder where the Kaspersky Industrial CyberSecurity for Nodes msi file is stored:

```
msiexec /i kics_win.msi/l*v kics.log /qn EULA=1 PRIVACYPOLICY=1
```

To install the Kaspersky Industrial CyberSecurity for Nodes Console:

```
msiexec /i kicstools.msi /qn EULA=1
```

To install and activate Kaspersky Industrial CyberSecurity for Nodes using the key file C:\0000000A.key and configure Kaspersky Industrial CyberSecurity for Nodes according to the settings in the configuration file C:\settings.xml:

```
msiexec /i kics_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

To install an application patch when Kaspersky Industrial CyberSecurity for Nodes is password-protected:

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation

Kaspersky Industrial CyberSecurity for Nodes starts protection and scan tasks immediately after installation if you have activated the application. If the **Enable Real-Time File Protection after installation of application (recommended)** check box is selected during installation of Kaspersky Industrial CyberSecurity for Nodes, the application scans the device's file system objects when they are accessed. If the Script monitoring component was installed as part of custom installation, Kaspersky Industrial CyberSecurity for Nodes scans the source code of all scripts when they are started. Kaspersky Industrial CyberSecurity for Nodes will run the *Critical Areas Scan* task every Friday at 8:00 P.M.

We recommend that you take the following steps after installing Kaspersky Industrial CyberSecurity for Nodes:

- Start the Kaspersky Industrial CyberSecurity for Nodes Update task. After installation Kaspersky Industrial CyberSecurity for Nodes will scan objects using the database included in its distribution kit. We recommend that you update the Kaspersky Industrial CyberSecurity for Nodes database immediately. To do this, run the *Update* task. The update will then run every hour according to the default schedule.

  For example, you can start the *Update* task by running the following command:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  In this case, Kaspersky Industrial CyberSecurity for Nodes database updates are downloaded from Kaspersky update servers.

- Start the *Critical Areas Scan* task if no anti-virus software with real-time file protection was installed on the device before installation of Kaspersky Industrial CyberSecurity for Nodes.

  You can start the *Critical Areas Scan* task from the command line by running the following command:

  ```
  KAVSHELL SCANCRITICAL /W:scancritical.log
  ```

  This command saves the task log in a file named scancritical.log contained in the current folder.

- Configure administrator notifications about Kaspersky Industrial CyberSecurity for Nodes events.

Adding / removing components. Sample commands

The On-Demand Scan component is installed automatically. You do not need to specify it in the list of ADDLOCAL key values by adding or deleting Kaspersky Industrial CyberSecurity for Nodes components.

To add the Applications Launch Control component to the components that have already been installed, run the following command:

```
msiexec /i kics_win.msi ADDLOCAL=Oas,AppCtrl /qn
```

or

```
\exec\setup_kics.exe /s /p ADDLOCAL=Oas,AppCtrl
```

If you list the components you want to install along with the already installed components, Kaspersky Industrial CyberSecurity for Nodes will reinstall the existing components.

To remove installed components run the following command:

```
msiexec /i kics_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,Bases,Core,CoreBLFiles,CoreFolders,CoreWPFiles,DevCtrl,Driver
ADD_ADV=IDS,RegMonitor REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Kaspersky Industrial CyberSecurity for Nodes uninstallation. Sample commands

To uninstall Kaspersky Industrial CyberSecurity for Nodes from the protected device in silent mode, run the following command:

```
msiexec /x kics_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

or

```
msiexec /x {DF1C0C50-2E34-4B22-A07D-133E3DC961C7} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

or

```
setup_kics.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

where `<user name>` is the name and login of a user with sufficient rights to uninstall.

If an empty Windows password is set for the user account that performs the removal, disable the **Request password to confirm critical actions** functionality before starting the removal.

To uninstall the Kaspersky Industrial CyberSecurity for Nodes Console in silent mode, run the following command:

```
msiexec /x kicstools.msi /qn
```

or

```
msiexec /x {5209F134-35AD-4A12-85B9-257FA5B52917} /qn
```

Return codes

The application installer can return the return codes described in this article.

The table below contains a list of command-line return codes.

Return codes

Code	Description
27100	Drives with Authentication Agent installed in test mode have been detected on the computer.
27101	Drives with Authentication Agent installed in test mode have been detected on the computer.
27102	Failed to find encrypted disks.
27200	Failed to unload application from RAM.
27201	Error while starting the AVP.exe process. Your computer may be infected.
27204	Failed to cache distributive package.
27205	Failed to migrate license information.
27206	Failed to remove license information.
27207	Failed to remove incompatible software.
27208	Failed to check incompatible software.
27209	Failed to extract files from cabinet.
27210	Failed to configure Self-Defense.
27211	Failed to enable Self-Defense.
27212	Failed to get operating system version info.
27213	Failed to get startup directory.
27214	Failed to verify installation directory.
27215	Failed to configure service.
27216	Failed to configure klcp upgrade.

Code	Description
27217	Failed to upgrade klcp.
27218	Failed to configure kl1 driver parameters.
27219	Failed to configure klelam driver parameters.
27220	Failed to configure klwfp driver parameters.
27221	Failed to configure driver compatibility mode.
27222	Failed to remove registry key.
27223	Failed to restart operating system.
27224	Failed to install driver.
27225	Failed to migrate driver settings.
27226	Failed to stop driver.
27227	Failed to block driver start.
27228	Failed to verify the signature of the file.
27230	Failed to prepare kldl driver settings.
27231	Failed to configure kldl driver settings.
27300	Error installing driver.
27301	Error removing driver.
27302	Error installing network components.
27303	Registration information for the driver is inconsistent or incomplete. Please restart the operating system and try again.
27305	Error disabling driver.
27310	Failed to install digitally signed catalog file.
27311	Failed to uninstall digitally signed catalog file.
27312	Failed to install certificates.
27313	Failed to remove certificates.
27320	Failed to configure service.
27321	Failed to unprotect service.
27350	Patch <patch name> is not intended for the <application name> application localization.
27352	Full disk encryption patch cannot be removed.
27353	Patch <patch 1 name> can be installed only together with patch <patch 2 name>.
27354	The computer must be restarted to apply the patches before the application is modified/restored.
27355	Failed to lock Full Disk Encryption management. Failed to lock Full Disk Encryption management. You must finish encryption to install an update for Full Disk Encryption.
27356	Patch cannot be installed.
27357	Installation package has been found to contain recalled patches. Installation will be aborted.
27360	Patch cannot be registered.
27361	Failed to set patch installation parameters.
27363	The patch contains encryption libraries that are incompatible with the installed encryption libraries.
27370	Error initializing .NET 8.0 unpacking.
27371	Error unpacking .NET 8.0.
27372	Registration information about the previous application version was deleted. Please restart the installation.
27373	Failed to delete registration information about the previous application version.
27374	The application is upgrading. Please try again later.

Code	Description
27375	Uninstallation password or user name has not been specified or is incorrect.
27376	Failed to uninstall Kaspersky Endpoint Agent. Please uninstall it yourself or disable password protection in settings. Then restart the installation of the application.
27377	Failed to uninstall Kaspersky Security for Windows Server. Please uninstall it yourself or disable password protection in settings. Then restart the installation of the application.
27378	Out of disk space.
27379	Failed to install the application because the incompatible components were selected. Please change the set of components and restart the installation.
27380	An invalid configuration file has been selected.
27381	An invalid license key has been selected.
27382	Failed to create the application administration group.
27383	You have selected an invalid folder. The name of the destination folder cannot exceed 160 characters.
27384	You have selected an invalid folder or drive. The application must be installed on a local hard drive.
27385	You have selected an invalid folder. The application cannot be installed to the root folder.
27386	You have selected an invalid folder. The application cannot be installed to the Windows folder or its subfolders.
27387	You have selected an invalid folder. The application cannot be installed to a folder that contains a Temp subfolder.
27388	You have selected an invalid folder. The application cannot be installed directly in the Program Files folder.
27389	You have selected an invalid folder. The application cannot be installed on a virtual disk.
27390	You have selected an invalid folder or drive. The application cannot be installed to the folder where the previous version of the application is installed.
27391	The selected folder or drive already contains files. The application cannot be installed to a folder that contains other data, because this data can become unavailable after Self-Defense is enabled.
27392	The application cannot be installed to a folder that contains Reparse Points. Please select another installation folder.
27393	The application cannot be installed to a folder that contains a semicolon (;) in its name. Please select another installation folder.
27394	You have selected an invalid folder. The root folder cannot be specified.
27395	You have selected an invalid folder. The Windows folder or its subfolders cannot be specified.
27396	You have selected an invalid folder. The Program Files folder cannot be specified directly.
27397	You have selected an invalid folder. A folder that contains a Temp subfolder cannot be specified.
27400	Error initializing file updates.
27450	CAB file could not be installed.
27451	Error removing.
27452	Error removing files.
27453	Error moving files.
27454	Failed to create registry files.
27455	Failed to get operating system version info.
27456	Failed to schedule rollback registry values.
27457	Failed to get well-known security identifiers (SIDs).
27460	Error creating security descriptors.
27461	Error restoring security descriptors.
27462	Failed to create rules for Microsoft Windows Firewall.
27463	Failed to delete rules for Microsoft Windows Firewall.

Installing and uninstalling the application using Kaspersky Security Center

This section contains information about installing Kaspersky Industrial CyberSecurity for Nodes using Kaspersky Security Center, a description of the procedure for installing and uninstalling Kaspersky Industrial CyberSecurity for Nodes through Kaspersky Security Center, and a description of actions to be taken after Kaspersky Industrial CyberSecurity for Nodes is installed.

General information about installing via Kaspersky Security Center

You can install Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Industrial CyberSecurity for Nodes will be installed with identical settings on multiple protected devices.

All protected devices can be combined in a single administration group, and a group task can be created to install Kaspersky Industrial CyberSecurity for Nodes on the protected devices in this group.

You can create a task to remotely install Kaspersky Industrial CyberSecurity for Nodes on a set of protected devices that are not in the same administration group. When creating this task, you must generate the list of individual protected devices that Kaspersky Industrial CyberSecurity for Nodes should be installed on.

Detailed information on the remote installation task is provided in Kaspersky Security Center Help.

Rights to install or uninstall Kaspersky Industrial CyberSecurity for Nodes

The account specified in the remote installation (removal) task must be included in the administrators group on each of the protected devices in all cases except those described below:

- If the Kaspersky Security Center Network Agent is already installed on the protected devices on which Kaspersky Industrial CyberSecurity for Nodes is to be installed (regardless of which domain the protected devices are in or whether they belong to any domain).

  If the Network Agent is not yet installed on the protected devices, you can install it with Kaspersky Industrial CyberSecurity for Nodes using a remote installation task. Before installing the Network Agent, make sure that the account you want to specify in the task is included in the administrators group on each of the protected devices.

- All protected devices on which you want to install Kaspersky Industrial CyberSecurity for Nodes are in the same domain as the Administration Server, and the Administration Server is registered as the **Domain Admin** account (if this account has local administrator rights on the protected devices within the domain).

By default, when using the **Forced installation** method, the remote installation task is run from the account running the Administration Server.

When working with group tasks or with tasks for sets of protected devices under forced installation (uninstallation) mode, an account must have the following rights on the protected device:

- Right to execute applications remotely.
- Rights to the **Admin$** share.
- Right to **Log on as a service**.

Installing Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center

Installing Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center involves the following steps:

1. **Creating an installation package**

   An *installation package* is a set of files created for remote installation of a Kaspersky application via Kaspersky Security Center. The installation package contains a range of settings needed to install the application and get it running immediately after installation. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

   How to create an installation package in the Kaspersky Security Center Administration Console

   1. In the Kaspersky Security Center Administration Console tree, select the **Advanced** → **Remote installation** → **Installation packages** folder.
   2. In the results pane, click the **Create installation package** button.

   The New Package Wizard starts. Follow the instructions of the Wizard.

   ### Step 1. Selecting the installation package type

   Select the **Create an installation package for a Kaspersky application** option.

   ### Step 2. Defining the installation package name

   Enter the name of the installation package, for example, *Kaspersky Industrial CyberSecurity for Nodes*.

   ### Step 3. Selecting the distribution package for installation

   Specify the kics_win.kud file from the Kaspersky Industrial CyberSecurity for Nodes distribution kit as the installation package file.

If necessary, select the **Copy updates from repository to installation package** check box to update the anti-virus databases in the installation package.

Step 4. End User License Agreement and Privacy Policy

If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select the **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes.

> You must accept the License Agreement and the Privacy Policy to proceed.

The installation package will be created and added to Kaspersky Security Center. Using the installation package, you can install Kaspersky Industrial CyberSecurity for Nodes on corporate network computers or update the application version.

To change the set of Kaspersky Industrial CyberSecurity for Nodes components to be installed and the default installation settings in the created installation package:

1. In the Kaspersky Security Center Administration Console expand the **Remote installation** node.
2. In the results pane of the **Installation packages** child node, open the context menu of the created Kaspersky Industrial CyberSecurity for Nodes installation package and select **Properties**.
3. In the **Properties: <name of installation package>** window open the **Settings** section.
4. Select the type of application installation:

   If the **Protect computer with Anti-Virus Bases** configuration is selected, all Kaspersky Industrial CyberSecurity for Nodes components are included by default except the Firewall and Performance Counters components.

   When you install the **Protect computer with Anti-Virus Bases** configuration of application over an application version that does not use signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically extended by adding the following components:

   - Real-Time File Protection
   - On-Demand Scan
   - Network Threat Protection

   > The components enabling updates are not included in the **Protect computer with Default Deny technology** configuration.

If the **Protect computer with Default Deny technology** configuration is selected, the following components are included by default:

- Exploit Prevention
- Applications Launch Control
- System Tray Icon

When you install the **Protect computer with Default Deny technology** configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components:

- Real-Time File Protection
- On-Demand Scan
- Components enabling updates

This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.

- **Full functionality**

  By default, all Kaspersky Industrial CyberSecurity for Nodes components other than Performance Counters and Endpoint Agent, are among those recommended for installation.

  The SNMP Protocol Support component of Kaspersky Industrial CyberSecurity for Nodes will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the protected device.

- **Endpoint Agent**

  When you select this option, Kaspersky Industrial CyberSecurity for Nodes is installed in the Endpoint Agent configuration. For detailed information about this configuration, see this section.

5. Specify the list of exclusions for industrial systems by clicking the **Configure** button.

6. In the **Component selection** block, select the check boxes next to the names of the Kaspersky Industrial CyberSecurity for Nodes components you want to install.

7. In the **Real-Time File Protection mode** block, select the **Enable Real-Time File Protection after installation of application (recommended)** check box and select the component operating mode.

8. If necessary, change the TCP port numbers that the Application Console uses for the remote connection to the computer with the application installed.

   The default port number for connection with Windows credentials is 13032, and the default port number for connection with credentials of manually created users is 13031. Range of possible port numbers: 1–65535.

   To prevent connection with credentials of manually created user accounts, clear the **Using credentials from manually created users** check box.

9. In order to indicate an installation folder other than the default one, specify the folder name and path in the **Configure application installation paths** block, by clicking the **Settings** button.

10. To install the application with predefined settings, upload the configuration file.

11. Save your changes.

How to create an installation package in the Web Console

1. Do one of the following:

   - In the main window of the Web Console, select **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   - In the main window of the Web Console, select **Operations** → **Repositories** → **Installation packages**.

   This opens a list of installation packages that have been downloaded to Kaspersky Security Center.

2. Click **Add**.

   The New Package Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting the installation package type

Select the **Create an installation package for a Kaspersky application** option.

The Wizard will create an installation package from the distribution package residing on Kaspersky servers. The list is updated automatically as new versions of applications are released.

You can also create an installation package from a file.

Step 2. Installation packages

Select the Kaspersky Industrial CyberSecurity for Nodes installation package. The installation package creation process starts. During creation of the installation package, you must accept the terms of the End User License Agreement and Privacy Policy.

> You must accept the License Agreement and the Privacy Policy to proceed.

The installation package will be created and added to Kaspersky Security Center. Using the installation package, you can install Kaspersky Industrial CyberSecurity for Nodes on corporate network computers or update the application version.

To change the set of Kaspersky Industrial CyberSecurity for Nodes components to be installed and the default installation settings in the created installation package:

1. In the **Installation packages** window, click on the name of the created Kaspersky Industrial CyberSecurity for Nodes installation package.

2. In the window that opens, select the **Settings** tab.

3. Select the **Protection components** section.

4. Select the type of application installation:

   If the **Protect computer with Anti-Virus Bases** configuration is selected, all Kaspersky Industrial CyberSecurity for Nodes components are included by default except the Firewall and Performance Counters components.

   When you install the **Protect computer with Anti-Virus Bases** configuration of application over an application version that does not use signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically extended by adding the following components:

   - Real-Time File Protection
   - On-Demand Scan
   - Network Threat Protection

   > The components enabling updates are not included in the **Protect computer with Default Deny technology** configuration.

   If the **Protect computer with Default Deny technology** configuration is selected, the following components are included by default:

   - Exploit Prevention
   - Applications Launch Control
   - System Tray Icon

   When you install the **Protect computer with Default Deny technology** configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components:

   - Real-Time File Protection
   - On-Demand Scan
   - Components enabling updates

   This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.

   - **Full functionality**

     By default, all Kaspersky Industrial CyberSecurity for Nodes components other than Performance Counters and Endpoint Agent, are among those recommended for installation.

     The SNMP Protocol Support component of Kaspersky Industrial CyberSecurity for Nodes will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the protected device.

   - **Endpoint Agent**

     When you select this option, Kaspersky Industrial CyberSecurity for Nodes is installed in the Endpoint Agent configuration. For detailed information about this configuration, see this section.

5. Specify the list of exclusions for industrial systems by clicking the **Configure** button.

6. In the **Select components to install** section, select the check boxes next to the names of the Kaspersky Industrial CyberSecurity for Nodes components you want to install.

7. In the **Real-Time File Protection mode** block, select the **Enable Real-Time File Protection after installation of application (recommended)** check box and select the component operating mode.

8. If necessary, change the TCP port numbers that the Application Console uses for the remote connection to the computer with the application installed.

   The default port number for connection with Windows credentials is 13032, and the default port number for connection with credentials of manually created users is 13031. Range of possible port numbers: 1–65535.

   To prevent connection with credentials of manually created user accounts, clear the **Port for remote connection using credentials from manually created users** check box.

9. Select the **Installation settings** section.

10. In the **Advanced Settings** section, configure the following settings:

    - **Add application location to environment variable %PATH%**. You can add the installation path to the %PATH% variable for convenient application management from the command line.

    - **Perform recommended action during scan at OS startup**. If this check box is selected, the *Scan at Operating System Startup* task runs in the **Perform recommended action** mode.

    - **Use low resource consumption mode for Kaspersky Security Center Network Agent**. Power saving mode allows you to limit the amount of RAM that Network Agent uses on the protected device. By default, power saving mode is disabled.

    - **Display System Tray Icon in the taskbar**. If the check box is selected, after Kaspersky Industrial CyberSecurity for Nodes is installed, the application icon appears in the Microsoft Windows taskbar notification area.

11. If necessary, disable the **Protect the installation process** functionality.

12. If necessary, change the default folders that are created on the protected device during application installation.

13. To install the application with predefined settings, click the **Add configuration file** link and upload the configuration file.

    When working with installation packages in Kaspersky Security Center Web Console, the maximum supported size of uploaded configuration files is 4 MB. If you work with installation packages in the Kaspersky Security Center Administration Console, this limit does not apply.

14. Save your changes.

2 Creating a remote installation task

The *Install application remotely* task allows you to remotely install Kaspersky Industrial CyberSecurity for Nodes. The *Install application remotely* task allows you to deploy the installation package of the application to all computers in the organization.

How to create a remote installation task in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Tasks**.

   The list of tasks opens.
3. Click **New task**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Security Center Administration Server → Install application remotely**.

Step 2. Selecting an installation package

Select Kaspersky Industrial CyberSecurity for Nodes installation package from the list. If the list does not contain the installation package for Kaspersky Industrial CyberSecurity for Nodes, you can create the package in the Wizard.

You can configure the installation package settings in Kaspersky Security Center. For example, you can select the application components that will be installed to a computer.

Network Agent will also be installed together with Kaspersky Industrial CyberSecurity for Nodes. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

Step 3. Additional

Select the Network Agent installation package. The selected version of Network Agent will be installed together with Kaspersky Industrial CyberSecurity for Nodes.

Step 4. Settings

Configure the following additional application settings:

- **Force installation package download**. Select the method of application installation:
  - **Using Network Agent**. The Network Agent is responsible for delivering the Kaspersky Industrial CyberSecurity for Nodes installation package to the client computers. If the Network Agent is not installed, the task will end with an error. In this case, add the Network Agent installation package to the *Install application remotely* task and enable file delivery via operating system resources. Then the Network Agent will be installed using operating system resources. Kaspersky Industrial CyberSecurity for Nodes is then installed using Network Agent.
  - **Using operating system resources through distribution points**. The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to the Kaspersky Security Center Help.
  - **Using operating system resources through Administration Server**. Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Behavior for devices managed through other Administration Servers**. Select the Kaspersky Industrial CyberSecurity for Nodes installation method. If the network has more than one Administration Server installed, these Administration Servers may see the same client computers. This may cause, for example, an application to be installed remotely on the same client computer several times through different Administration Servers, or other conflicts.
- **Do not re-install application if it is already installed**. Clear this check box if you want to install an earlier version of the application, for example.

Step 5. Selecting the operating system restart setting

Select the action to be performed if a computer restart is required. A restart is not necessary when installing Kaspersky Industrial CyberSecurity for Nodes. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.

Step 6. Selecting the devices to which the task will be assigned

Select the computers on which Kaspersky Industrial CyberSecurity for Nodes will be installed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. Network Agent is not installed on unassigned devices. In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 7. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Industrial CyberSecurity for Nodes using Network Agent tools, you do not have to select an account.

Step 8. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 9. Defining the task name

Enter a name for the task, for example, *Installing Kaspersky Industrial CyberSecurity for Nodes for Windows 5.0*.

Step 10. Finishing task creation

Finish the wizard. If necessary, select the **Run the task after the wizard finishes** check box. You can monitor the progress of the task in the task properties. The application will be installed in silent mode. After installation, the icon will be added to the notification area of the user's computer. If the icon looks like this , make sure that you activated the application.

How to create a remote installation task in the Web Console

1. In the main window of the Web Console, select **Asset management → Tasks**.

   The list of tasks opens.

2. Click **Add**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Security Center**.
2. In the **Task type** drop-down list, select **Install application remotely**.
3. In the **Task name** field, enter a brief description, such as *Installation of Kaspersky Industrial CyberSecurity for Nodes for Managers*.
4. In the **Devices to which the task will be assigned** block, select the task scope.

Step 2. Selecting computers for installation

At this step, select the computers on which Kaspersky Industrial CyberSecurity for Nodes will be installed according to the selected task scope option.

Step 3. Configuring an installation package

At this step, configure the installation package:

1. Select the Kaspersky Industrial CyberSecurity for Nodes for Windows (5.0) installation package.
2. Select the Network Agent installation package.

   The selected version of Network Agent will be installed together with Kaspersky Industrial CyberSecurity for Nodes. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

3. In the **Force installation package download** block, select the application installation method:

   - **Using Network Agent**. The Network Agent is responsible for delivering the Kaspersky Industrial CyberSecurity for Nodes installation package to the client computers. If the Network Agent is not installed, the task will end with an error. In this case, add the Network Agent installation package to the *Install application remotely* task and enable file delivery via operating system resources. Then the Network Agent will be installed using operating system resources. Kaspersky Industrial CyberSecurity for Nodes is then installed using Network Agent.

   - **Using operating system resources through distribution points**. The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to the Kaspersky Security Center Help.

   - **Using operating system resources through Administration Server**. Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.

4. In the **Maximum number of concurrent downloads** field, set a limit on the number of installation package download requests sent to the Administration Server. A limit on the number of requests will help prevent the network from being overload.

5. In the **Maximum number of installation attempts** field, set a limit on the number of attempts to install the application. If installation of Kaspersky Industrial CyberSecurity for Nodes ends with an error, the task will automatically start the installation again.

6. If necessary, clear the **Do not re-install application if it is already installed** check box. It allows, for example, to install one of the previous versions of the application.

7. If necessary, clear the **Verify operating system type before downloading** check box. This lets you avoid downloading an application distribution package if the operating system of the computer does not meet the software requirements. If you are sure that the operating system of the computer meets the software requirements, you can skip this verification.

8. If necessary, select the **Assign package installation in Active Directory group policies** check box. Kaspersky Industrial CyberSecurity for Nodes is installed by means of Network Agent or manually by means of Active Directory. To install Network Agent, the remote installation task must be run with domain administrator privileges.

9. If necessary, select the **Prompt users to close running applications** check box. Installation of Kaspersky Industrial CyberSecurity for Nodes takes up computer resources. For the convenience of the user, the Application Installation Wizard prompts you to close running applications before starting the installation. This helps prevent disruptions in the operation of other applications and prevents possible malfunctions of the computer.

10. In the **Behavior for devices managed through other Administration Servers** block, select the Kaspersky Industrial CyberSecurity for Nodes installation method. If the network has more than one Administration Server installed, these Administration Servers may see the same client computers. This may cause, for example, an application to be installed remotely on the same client computer several times through different Administration Servers, or other conflicts.

Step 4. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Industrial CyberSecurity for Nodes using Network Agent tools, you do not have to select an account.

Step 5. Completing task creation

Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks. To run a task, select the check box opposite the task and click the **Start** button. The application will be installed in silent mode. After installation, the icon will be added to the notification area of the user's computer. If the icon looks like this , make sure that you activated the application.

Detailed information about generating an installation package and creating a remote installation task is provided in the Kaspersky Security Center Help.

Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation

After you install Kaspersky Industrial CyberSecurity for Nodes, we recommend that you update Kaspersky Industrial CyberSecurity for Nodes databases on the devices, and perform a Critical Areas Scan of the devices if no anti-virus applications with enabled real-time protection were installed on the devices before installation of Kaspersky Industrial CyberSecurity for Nodes.

If the protected devices on which Kaspersky Industrial CyberSecurity for Nodes was installed are part of the same administration group in the Kaspersky Security Center, you can perform these tasks using the following methods:

1. Create the *Update* task for the group of protected devices on which Kaspersky Industrial CyberSecurity for Nodes was installed. Set the Kaspersky Security Center Administration Server as the update source.

2. Create an On-Demand Scan group task with the *Critical Areas Scan* status. Kaspersky Security Center evaluates the security status of each protected device in the group based on the results of this task, not based on the results of the *Critical Areas Scan* task.

3. Create a new policy for the group of protected devices. In the policy properties, in the **Application Settings** section, deactivate the scheduled start of local system on-demand scan tasks and the *Update* tasks on the administration group's protected devices in the settings of the **Run local system tasks** subsection.

You can also configure administrator notifications about Kaspersky Industrial CyberSecurity for Nodes events.

Installing the Application Console via Kaspersky Security Center

Detailed information about creating an installation package and a remote installation task is provided in the Kaspersky Security Center Help.

To install the Application Console using a remote installation task:

1. In the Kaspersky Security Center Administration Console expand the **Advanced** node.
2. Expand the **Remote installation** child node.
3. Create an installation package:
   a. In the results pane of the **Installation packages** child node, click the **Create installation package** button.
   b. In the **New Package Wizard** window, select **Create installation package for specified executable file** as a package type.
   c. Enter the new installation package name.
   d. Select the \client\setup_kicstool.exe file from the Kaspersky Industrial CyberSecurity for Nodes distribution kit folder and select the **Copy entire folder to the installation package** check box.
   e. In the **Executable file launch settings (optional)** field, specify the parameter values EULA=1 and PRIVACYPOLICY=1:

      ```
      /s /p "EULA=1 PRIVACYPOLICY=1"
      ```

      Otherwise, it is impossible to install components.
   f. If necessary, in the **Executable file launch settings (optional)** field, you can specify the ADDLOCAL command-line parameter to change the set of components to be installed, and the INSTALLDIR command-line parameter to specify a destination folder other than the default one. For example, to perform a standalone installation of the Application Console in the C:\KasperskyConsole folder, use the following command-line option:

      ```
      /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
      ```
4. In the **Installation packages** child node, create a task to remotely install the Application Console on the selected protected devices (administration group).
5. Configure the task settings.
6. Run the remote installation task.

The Application Console is installed on the protected devices specified in the task.

Uninstalling Kaspersky Industrial CyberSecurity for Nodes via Kaspersky Security Center

Dump and trace files are not deleted on uninstalling Kaspersky Industrial CyberSecurity for Nodes. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

If management of Kaspersky Industrial CyberSecurity for Nodes on network devices is password protected, enter the password when creating a task to uninstall multiple applications. If the password protection is not managed centrally by a Kaspersky Security Center policy, Kaspersky Industrial CyberSecurity for Nodes will be successfully uninstalled from the devices, on which the entered password matched the set value. Kaspersky Industrial CyberSecurity for Nodes will not be uninstalled from other protected devices.

To uninstall Kaspersky Industrial CyberSecurity for Nodes:

1. In the Kaspersky Security Center Administration Console, create and start an application removal task.
2. In the task, select the uninstallation method (similar to selecting the installation method; see the previous section) and specify the account that Administration Server will use to access the protected devices. You can uninstall Kaspersky Industrial CyberSecurity for Nodes with only the default uninstallation settings.

Changing the set of application components using Kaspersky Security Center

The *Change application components* task allows you to change the set of components of Kaspersky Industrial CyberSecurity for Nodes after the application is installed.

How to change the set of application components in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Tasks**.

   The list of tasks opens.

2. Click **New task**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Industrial CyberSecurity for Nodes (5.0) → Change application components**.

Step 2. Task settings for changing application components

Select the application components that will be available on the user's computer. Configure the advanced settings for the task (see the table below).

When modifying the application configuration to use the Endpoint Agent for MDR, ensure that all components responsible for receiving telemetry are enabled.

Step 3. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 4. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 5. Defining the task name

Enter a name for the task, for example, *Add the Application Control component*.

Step 6. Completing task creation

Finish the wizard. If necessary, select the **Run the task after the wizard finishes** check box. You can monitor the progress of the task in the task properties.

How to change the set of application components in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

   The list of tasks opens.

2. Click **Add**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.
2. In the **Task type** drop-down list, select **Change Kaspersky Industrial CyberSecurity for Nodes components**.
3. In the **Task name** field, enter a brief description, for example, *Add the Application Control component*.
4. In the **Devices to which the task will be assigned** block, select the task scope.

Step 2. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. For example, select a separate administration group or build a selection.

Step 3. Completing task creation

1. Select the **Open task details when creation is complete** check box and finish the wizard.
2. In the task properties, select the **Application settings** tab.
3. Select the application components that will be available on the user's computer. Configure the advanced settings for the task (see the table below).

> When modifying the application mode to use the Endpoint Agent for MDR, ensure that all components responsible for receiving telemetry are enabled.

As a result, the set of Kaspersky Industrial CyberSecurity for Nodes components on users' computers will be changed in silent mode.

Advanced task settings

Parameter	Description
Industrial software exclusion profile	For the *Change application components* task, you can only add exclusions from scanning and trusted applications to the trusted zone.
Use password for modifying the set of application components	Administrators typically enable Password protection to restrict access to Kaspersky Industrial CyberSecurity for Nodes. That is, to modify the selection of application components, you must enter credentials of a user that has the **Remove / modify / restore the application** permission. For example, you can use the KLAdmin account.

Parameter	Description
Check for incompatible third-party applications	By default, Kaspersky Industrial CyberSecurity for Nodes checks installed applications for compatibility. The list of incompatible software is available in the incompatible.txt file that is included in the distribution kit. If the incompatible software check is enabled, Kaspersky Industrial CyberSecurity for Nodes stops the task upon detecting an application from the list. You can disable the scan of installed software if the vendor documentation of the third-party software claims compatibility with Endpoint Protection Platform (EPP).
Remove incompatible third-party applications	Automatic removal of applications from the incompatible.txt list before changing the set of components. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes attempts to remove the applications that may cause compatibility issues in order to continue the task. This option is enabled by default.

Installing and uninstalling the application via Active Directory group policies

This section describes how to install and uninstall Kaspersky Industrial CyberSecurity for Nodes through Active Directory group policies, as well as information on the actions that must be performed after installing Kaspersky Industrial CyberSecurity for Nodes through group policies.

Installing Kaspersky Industrial CyberSecurity for Nodes via Active Directory group policies

You can install Kaspersky Industrial CyberSecurity for Nodes on several protected devices via the Active Directory group policy. You can install the Application Console the same way.

The protected devices on which you want to install Kaspersky Industrial CyberSecurity for Nodes or the Application Console must be in the same domain and a single organizational unit.

The operating systems on the protected devices on which you want to install Kaspersky Industrial CyberSecurity for Nodes using the policy must be of the same bitness (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Industrial CyberSecurity for Nodes, use the kics_win.msi installation package. To install the Application Console, use the kicstools.msi installation package.

Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

To install Kaspersky Industrial CyberSecurity for Nodes or the Application Console:

1. Save kics_win.msi to a shared folder on the domain controller.
2. Save the key file in the same public folder on the domain controller.
3. In the same shared folder on the domain controller, create an install_props.json file that contains the lines below. This signifies that you agree to the terms of the End User License Agreement and Privacy Policy.

```
{
"EULA": "1",
```

```
"PRIVACYPOLICY": "1"
}
```

4. On the domain controller create a new policy for the group that the protected devices belong to.

5. Using the **Group Policy Object Editor**, create a new installation package in the **Computer Configuration** node. Specify the path to the msi file for Kaspersky Industrial CyberSecurity for Nodes (or Application Console) in UNC (Universal Naming Convention) format.

6. Select the Windows Installer's **Always install with elevated privileges** check box in both the **Computer Configuration** node and in the **User Configuration** node of the selected group.

7. Apply the changes using the `gpupdate / force` command.

Kaspersky Industrial CyberSecurity for Nodes will be installed on the protected devices of the group after they have been restarted.

Actions to perform after Kaspersky Industrial CyberSecurity for Nodes installation

After installing Kaspersky Industrial CyberSecurity for Nodes on the protected devices, it is recommended that you immediately update the application databases and run a Critical Areas scan. You can perform these actions from the Application Console.

You can also configure administrator notifications about Kaspersky Industrial CyberSecurity for Nodes events.

Uninstalling Kaspersky Industrial CyberSecurity for Nodes via Active Directory group policies

Dump and trace files are not deleted on uninstalling Kaspersky Industrial CyberSecurity for Nodes. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

If you used an Active Directory group policy to install Kaspersky Industrial CyberSecurity for Nodes (or the Application Console) on the group of protected devices, you can use this policy to uninstall Kaspersky Industrial CyberSecurity for Nodes (or the Application Console).

You can uninstall the application only with the default uninstallation parameters.

Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

If application management is password protected, you cannot uninstall Kaspersky Industrial CyberSecurity for Nodes using Active Directory group policies.

To uninstall Kaspersky Industrial CyberSecurity for Nodes (or the Application Console):

1. On the domain controller, select the organizational unit from whose protected devices you want to uninstall Kaspersky Industrial CyberSecurity for Nodes or the Application Console.

2. Select the policy created for the installation of Kaspersky Industrial CyberSecurity for Nodes and in the **Group Policies Object Editor**, in the **Software installation** node (**Computer Configuration** > **Software Settings** > **Software installation**) open the context menu of the Kaspersky Industrial CyberSecurity for Nodes (or the Application Console) installation package and select the **All tasks** > **Remove** command.

3. Select the uninstallation method **Immediately uninstall the software from users and computers**.

4. Apply the changes using the `gpupdate /force` command.

Kaspersky Industrial CyberSecurity for Nodes is removed from the protected devices after they are restarted and before logging in to Microsoft Windows.

Kaspersky Industrial CyberSecurity for Nodes install and uninstall logs

If you install (uninstall) Kaspersky Industrial CyberSecurity for Nodes or Application Console using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. A log file named kl-install-<uid>.log (where <uid> is a unique 8-character log identifier) will be saved in the %temp% folder for the user whose account was used to start the setup_kics.exe or setup_kicstool.exe file.

If Kaspersky Industrial CyberSecurity for Nodes is installed or uninstalled from the command line, the install log file will not be created by default.

To install Kaspersky Industrial CyberSecurity for Nodes and create a log file on disk C:\, execute the following command:

```
msiexec /i kics_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

System changes after Kaspersky Industrial CyberSecurity for Nodes installation

When Kaspersky Industrial CyberSecurity for Nodes and the Kaspersky Industrial CyberSecurity for Nodes Console are installed together, the Windows Installer service will make the following modifications on the protected device:

- Kaspersky Industrial CyberSecurity for Nodes folders are created on the protected device and on the device where the Application Console is installed.

- Kaspersky Industrial CyberSecurity for Nodes services are registered.

- Kaspersky Industrial CyberSecurity for Nodes user group is created.

- Kaspersky Industrial CyberSecurity for Nodes keys are registered in the system registry.
- Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect system task that is displayed in the Windows Task Scheduler is created.
- Windows Firewall rules are created.

These changes are described below.

Kaspersky Industrial CyberSecurity for Nodes folders on a protected device

When Kaspersky Industrial CyberSecurity for Nodes is installed, the following folders are created on a protected device:

- Kaspersky Industrial CyberSecurity for Nodes default installation folder containing the Kaspersky Industrial CyberSecurity for Nodes executable files. The following installation folder is used by default:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
- Management Information Base (MIB) files containing a description of the counters and hooks published by Kaspersky Industrial CyberSecurity for Nodes via the SNMP protocol:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0\mibs
- Kaspersky Industrial CyberSecurity for Nodes service files:
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Data
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Settings
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Dskm
- Files with settings for update sources:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data
- Updates of databases and software modules downloaded using the *Update* task (the folder will be created the first time updates are downloaded using the *Update* task).

  %ProgramData%\Kaspersky Lab\KICS.5.0\Update distribution
- Task logs and system audit log:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Reports
- Set of databases currently in use:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Bases
- Backup copies of databases; they are overwritten each time the databases are updated:

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB
- Temporary files created during execution of update tasks:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data\temp\temporaryFolder

- Quarantined objects (default folder):
  %ProgramData%\Kaspersky Lab\KICS.5.0\QB
- Objects in backup (default folder):
  %ProgramData%\Kaspersky Lab\KICS.5.0\QB
- Objects restored from backup and quarantine (default folder for restored objects):
  %ProgramData%\Kaspersky Lab\KICS.5.0\QB\Restored

Folder created during installation of Application Console

The default installation folder of the Application Console depends on the operating system bit set. The following installation folder is used by default:

%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0

Kaspersky Industrial CyberSecurity for Nodes services

The following Kaspersky Industrial CyberSecurity for Nodes services run under the SYSTEM account:

- Kaspersky Industrial CyberSecurity for Nodes Service (AVP.KICS.5.0). The main system service of Kaspersky Industrial CyberSecurity for Nodes that protects devices against viruses and other threats
- Kaspersky Industrial CyberSecurity for Nodes Side-by-Side Service (AVP.KICS.5.0.SbS). The system service that protects the devices while Kaspersky Industrial CyberSecurity for Nodes is being updated, restored or undergoing component changes
- Kaspersky Seamless Update Service (avpsus.KICS.5.0). The system service that installs and rolls back critical and approved updates of application modules
- Kaspersky Industrial CyberSecurity for Nodes Remote Control Service (avpcos.KICS.5.0). The system service for remote restarting and stopping Kaspersky Industrial CyberSecurity for Nodes Service from Application Console

Kaspersky Industrial CyberSecurity for Nodes group

KICS Administrators is a group on the protected device, whose members have full access to all Kaspersky Industrial CyberSecurity for Nodes functions.

System registry keys

When Kaspersky Industrial CyberSecurity for Nodes is installed, the following system registry keys are created:

- Kaspersky Industrial CyberSecurity for Nodes settings:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.KICS.5.0]

- The Kaspersky Industrial CyberSecurity for Nodes event log (Kaspersky Event Log) parameters:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Industrial CyberSecurity for Nodes]

- Trace file settings:

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\Trace]

- Settings for application tasks and functions:

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment]

Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect system task

The Windows Installer service creates a Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect task during application installation. The task is started immediately after it is created and later at every OS startup. The task checks the version of the drivers used by the application: if an operating system version is updated, the application updates the drivers for the corresponding version of the operating system.

The task does not affect the application and can be deleted. We recommend to keep operating system upgrade scenario in mind.

Windows Firewall rules

Depending on the specified installation settings, Windows Firewall allow rules for incoming connections described in the table below can be created on the protected device.

Windows Firewall rules

Rule name	Rule description	Rule creation condition
AVP.KICS.5.0	Allow rule for the executable file avp.exe.	Always created.
AVP.KICS.5.0 Remote UI Connection	Allow rule for TCP port 13032.	Installing the application with the `ADDWFEXCLUSION=1` parameter.
AVP.KICS.5.0 Remote UI Connection	Allow rule for TCP port 13031. This port number is used by default. You can change the port number by specifying the `UIKLPORT=<port>` parameter. In this case, the application will create a rule for the specified port number.	Installing the application with the `ADDWFEXCLUSION=1` and `UIKLPORT=13031` parameters. The rule is not created if the `ENABLEUIKLPORT=0` parameter is passed

Rule name	Rule description	Rule creation condition
DHCP Discover In	Allow rule for UDP port 67.	Installing the application with the Integration with KICS for Networks component.
SSDP Discover In	Allow rule for UDP port 1900.	

Kaspersky Industrial CyberSecurity for Nodes processes

Kaspersky Industrial CyberSecurity for Nodes starts processes described in the table below.

Kaspersky Industrial CyberSecurity for Nodes processes

File name	Purpose
avp.exe	Kaspersky Industrial CyberSecurity for Nodes workflow
avpsus.exe	This process allows installing and rolling back critical and approved application module updates.

Checking Kaspersky Industrial CyberSecurity for Nodes functions. Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to check the Real-Time File Protection and On-Demand Scan features of Kaspersky Industrial CyberSecurity for Nodes.

About the EICAR test virus

This test virus is designed to verify the operation of anti-virus applications. It was developed by the European Institute for Computer Antivirus Research (EICAR).

The test virus is not a malicious object and does not contain executable code for your device, but most vendors' anti-virus applications identify it as a threat.

The file containing this test virus is called eicar.com. You can download it from the EICAR website.

Before saving the file in a folder on the device's hard drive, make sure that Real-Time File Protection is disabled on that drive.

The eicar.com file contains a line of text. When scanning the file Kaspersky Industrial CyberSecurity for Nodes detects the test threat in this line of text, assigns the **Infected** status to the file, and deletes it. Information about the threat detected in the file will appear in the Application Console and in the task log.

You can use the eicar.com file to check how Kaspersky Industrial CyberSecurity for Nodes disinfects the infected objects and how it detects probably infected objects. To do this, open the file using a text editor, add one of the prefixes listed in the table below to the beginning of the line of text in the file, and save the file with a new name, such as eicar_cure.com.

To make sure that Kaspersky Industrial CyberSecurity for Nodes processes the eicar.com file with a prefix, in the **Objects protection** security settings section, set the **All objects** value for the Real-Time Computer Protection tasks and Default On-Demand Scan tasks of Kaspersky Industrial CyberSecurity for Nodes.

Prefixes in EICAR files

Prefix	File status after the scan and Kaspersky Industrial CyberSecurity for Nodes action
No prefix	**Kaspersky Industrial CyberSecurity for Nodes assigns the Infected status to the object and deletes it.**
SUSP–	Kaspersky Industrial CyberSecurity for Nodes assigns the **Probably infected** status to the object detected by the heuristic analyzer and deletes it since probably infected objects are not disinfected.
WARN–	Kaspersky Industrial CyberSecurity for Nodes assigns the **Probably infected** status to the object (the object's code partly matches the code of a known threat) and deletes it since probably infected objects are not disinfected.
CURE–	Kaspersky Industrial CyberSecurity for Nodes assigns the **Infected** status to the object and disinfects it. If disinfection is successful, the entire text in the file is replaced with the word "CURE".

Checking the Real-Time File Protection and On-Demand Scan features

After installing Kaspersky Industrial CyberSecurity for Nodes, you can confirm that Kaspersky Industrial CyberSecurity for Nodes detects objects containing malicious code. To do this, use the EICAR test virus.

To check the Real-Time File Protection feature:

1. Download the eicar.com file from the EICAR website. Save it in a shared folder on the local drive of any device on the network.

   Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. If you want to check that network user notifications are working, make sure that the Microsoft Windows Messenger Service is enabled both on the protected device and on the device where you saved the eicar.com file.

3. Open the Application Console on the protected device.

4. Copy the saved eicar.com file to the local drive of the protected device using one of the following methods:

   - To test notifications through a Terminal Services window, copy the eicar.com file to the protected device after connecting to the protected device using the Remote Desktop Connection utility.

   - To test notifications through the Microsoft Windows Messenger Service, use the device's network places to copy the eicar.com file from the device where you saved it.

Real-Time File Protection is working as it should if the following conditions are met:

- The eicar.com file is deleted from the protected device.
- In the Application Console, the task log gets the *Critical* status. The log has a new line with information about a threat in the eicar.com file.
- The following Microsoft Windows Messenger Service message appears on the device from which you copied the file: Kaspersky Industrial CyberSecurity for Nodes blocked access to <path to file on the device>\eicar.com on computer <network name of the device> at <time that event occurred>. Reason: Threat detected. Virus: EICAR-Test-File. User name: <user name>. Computer name: <network name of the device from which you copied the file>.

  Make sure that the Microsoft Windows Messenger Service is running on the device from which you copied the eicar.com file.

To view the task log:

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the created On-Demand Scan task.
3. In the node results pane, click the **Open task log** link.

To check the On-Demand Scan feature:

1. Download the eicar.com file from the EICAR website. Save it in a shared folder on the local drive of any device on the network.

   Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. Open the Application Console and expand the **On-Demand Scan** node.
3. Select the **Critical Areas Scan** child node.
4. On the **Settings** tab for the scan scope, open the context menu of the **Network** node.
5. Select **Add network file**.
6. Enter the network path to the eicar.com file on the remote computer in UNC (Universal Naming Convention) format.
7. Select the check box to include the added network path in the scan scope.
8. Run the Critical Areas Scan task.

The On-Demand Scan is working as it should if the following conditions are met:

- The eicar.com file is deleted from the device's hard drive.
- In the Application Console, the task log gets the *Critical* status. The On-Demand Scan task log has a new line with information about a threat in the eicar.com file.

Upgrading older versions of Kaspersky Industrial CyberSecurity for Nodes to version 5.0

When upgrading an older version of Kaspersky Industrial CyberSecurity for Nodes to version 5.0, follow these recommendations:

- Plan ahead and schedule the upgrade. Choose a time when servers are operating under the lightest load, for example, during the weekend.
- After the upgrade, turn on application components one by one. That is, for example, start by enabling the Real-Time File Protection component alone, then enable other protection components, then enable control components, and so on. We recommend testing the application at each step.
- Carry out the upgrade step by step. First upgrade a single computer, then multiple computers, then upgrade all computers of the organization.

Steps of the upgrade procedure

Upgrade Kaspersky Industrial CyberSecurity for Nodes to version 5.0 in the following order:

1. **Upgrade Kaspersky Security Center**

   Upgrade all Kaspersky Security Center components to version 14.2 or higher, including Network Agent on user computers and Kaspersky Security Center Web Console.

2. **Upgrade the Kaspersky Industrial CyberSecurity for Nodes web plug-in**

   In the Kaspersky Security Center Web Console, upgrade the Kaspersky Industrial CyberSecurity for Nodes web plug-in to version 5.0.

3. **Migrate Kaspersky Industrial CyberSecurity for Nodes tasks and policies**

   After migrating policies and tasks, you must configure the settings that the migration wizard cannot migrate, and which did not exist in older versions of the application. We also recommend checking if the migration wizard correctly migrated all settings.

4. **Install Kaspersky Industrial CyberSecurity for Nodes 5.0**

   Kaspersky Industrial CyberSecurity for Nodes version 5.0 uses HTTPS protocol instead of DCOM protocol. Therefore, before installing the new version of Kaspersky Industrial CyberSecurity for Nodes, it is necessary to configure the device on which the application will be updated to enable remote start of the KICS service. If such configuration is not performed, remote service start will be unavailable.

   You can install Kaspersky Industrial CyberSecurity for Nodes 5.0 after removing an earlier version of the application or on top of it.

   When installing on top of an older version of the application, the same set of application components is installed, taking into account new names and contents of some components.

When installing remotely, the installer installs components that you select in the properties of the installation package.

5. **If necessary, activate Kaspersky Industrial CyberSecurity for Nodes 5.0**

   When installing Kaspersky Industrial CyberSecurity for Nodes 5.0 on top of an older version of the application, the current license is automatically applied to the application, and the new application components and tasks are fully available. The license term remains unchanged.

6. **Make sure the application is working**

   After upgrading Kaspersky Industrial CyberSecurity for Nodes, make sure that the application is working as intended. Make sure no errors are reported for the application, also check the time of the last connection to the Administration Server, the time of the last update and the computer protection status.

   Pay attention to the migration of exclusion lists, trusted applications, Device Control rules, and Applications Launch Control rules.

Updating Kaspersky Industrial CyberSecurity for Nodes

Upgrading to Kaspersky Industrial CyberSecurity for Nodes 5.0 is supported for versions 3.2 or later. To update from earlier versions of the application, you must remove the installed version and install version 5.0.

The update is performed by installing the new version of the application over the installed version of the application and does not require a computer restart.

By default, the application creates a new installation folder with the name of the new application version based on the path to the existing application installation folder. You can manually specify a new path for the application installation folder.

When upgrading Kaspersky Industrial CyberSecurity for Nodes to version 5.0, the previously installed version of the application is automatically deleted.

When updating a password-protected installation of Kaspersky Industrial CyberSecurity for Nodes, pass the password to the installer in one of the following ways:

- If installing locally via the Installation Wizard interface or in interactive CLI mode, specify the password when requested.
- If installing locally in non-interactive CLI mode, specify the password in the `UNLOCK_PASSWORD` key.
- If installing using Active Directory group policies, use the value of the `UNLOCK_PASSWORD` key in the install_props.json configuration file.

When the application that you are remotely upgrading via Kaspersky Security Center is password-protected, you must first disable password protection using a Kaspersky Security Center policy.

When updating the application, the current license is automatically applied to Kaspersky Industrial CyberSecurity for Nodes version 5.0, and the use of the new application components and tasks is fully available. The license term remains unchanged.

If an application is updated with an expired license, the new version of the application runs in limited functionality mode after installation (for example, application database updates are not available).

Updating Kaspersky Industrial CyberSecurity for Nodes Administration Tools

You can update the Administration Plug-in for managing the application using Kaspersky Security Center to version 5.0 only from versions 3.2, 4.0 or later. To update earlier versions of the Administration Plug-in and the Application Console, you must remove the installed version and then install version 5.0.

During the update a new version of the Administration Plug-in is installed next to the previously installed version and does not require a computer restart.

For information about migrating the settings of the Administration Plug-in, refer to this article.

Migrating policies and tasks

You can migrate policy and task settings of previous versions of the application to version 5.0 in the following ways:

- Using the Policies and Tasks Batch Conversion Wizard (only available in the Kaspersky Security Center Administration Console).
- Using the Kaspersky Industrial CyberSecurity for Nodes 5.0 Policies and Tasks Migration Wizard (available only in the Kaspersky Security Center Web Console).

It is recommended to begin with migrating policies and tasks of Kaspersky Industrial CyberSecurity for Nodes on a single computer, then do it on a group of computers, and then complete the migration on all computers of the organization.

How to use the Policies and Tasks Batch Conversion Wizard to migrate policy and task settings

1. In the Kaspersky Security Center Administration Console, select the Administration Server and open the context menu.
2. Select **All tasks → Policies and tasks batch conversion wizard**.

   This starts the Policies and Tasks Batch Conversion Wizard. Follow the instructions of the Wizard.

Step 1. Selecting the application for which you need to convert policies and tasks

Select Kaspersky Industrial CyberSecurity for Nodes 5.0. Go to the next step.

Step 2. Conversion of policies

Select the policies of the application version being upgraded that you want to create for Kaspersky Industrial CyberSecurity for Nodes 5.0.

Step 3. Migrating with the Kaspersky Endpoint Agent

If necessary, one by one, for each Kaspersky Industrial CyberSecurity for Nodes policy that you selected at the previous step of the wizard, select a Kaspersky Endpoint Agent policy whose settings you want to add to the new Kaspersky Industrial CyberSecurity for Nodes 5.0 policy. Go to the next step.

Step 4. Conversion of tasks

Select the group tasks of the application version being upgraded that you want to convert for Kaspersky Industrial CyberSecurity for Nodes 5.0.

Non-group tasks (tasks that are assigned to individual devices) are not displayed at the current step.

To convert non-group tasks from your version of the application to Kaspersky Industrial CyberSecurity for Nodes 5.0:

1. Click **Next**.

   The **Additionally migrate schedules and non-group tasks** window opens.

2. Select the **Migrate non-group tasks** check box.

3. Specify the connection settings for the Kaspersky Security Center Administration Server.

4. Click **OK**.

Step 5. Wizard completion

Finish the wizard. As a result, the wizard does the following:

- New policies for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  New policies contain settings from selected Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent policies and also new settings that were introduced in Kaspersky Industrial CyberSecurity for Nodes 5.0. The names of the new policies are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes policies before the conversion, with "(converted)" added. New policies has the *Inactive policy* status.

- New tasks for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  New tasks contain settings from the selected Kaspersky Industrial CyberSecurity for Nodes tasks and also new settings that were introduced in Kaspersky Industrial CyberSecurity for Nodes 5.0. The names of the new tasks are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes tasks before the conversion, with "(conversion)" added.

- Policies and tasks selected for conversion remain unchanged.

How to use the migration wizard to migrate policy and task settings

In the main window of the Web Console or Cloud Console select **Operations → Migration to Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.

This runs the policies and tasks migration wizard. Follow the instructions of the Wizard.

Step 1. Policy migration

Select Kaspersky Industrial CyberSecurity for Nodes and, if necessary, Kaspersky Endpoint Agent policies whose settings you want to merge.

Make sure you selected the correct policies and go to the next step.

Step 2. Task migration

Select the Kaspersky Industrial CyberSecurity for Nodes tasks that you want to create for Kaspersky Industrial CyberSecurity for Nodes 5.0.

Go to the next step.

Step 3. Wizard completion

Finish the wizard. As a result, the wizard does the following:

- New policies for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  New policies contain settings from migrated Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent policies and also new settings that were introduced in Kaspersky Industrial CyberSecurity for Nodes 5.0. The names of the new policies are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes policies before the merge, with the "copied from KICS" phrase added. New policies has the *Inactive policy* status.

- New tasks for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  New tasks contain settings from migrated Kaspersky Industrial CyberSecurity for Nodes tasks and also new settings that were introduced in Kaspersky Industrial CyberSecurity for Nodes 5.0. The names of the new tasks are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes tasks before the migration, with the "copied from KICS" phrase added.

Migration of settings of the application version being updated

The following is migrated without changes after upgrading of the application and its management plug-ins to version 5.0:

- Settings of components and tasks except those that are reset to defaults and those that are listed under "Limitations of settings and components migration"
- Task logs and system audit logs, as well as records in the Windows event log
- Task notification settings
- User accounts under which tasks are started
- User access permissions for application management
- Proxy server connection password
- Status of the attribute in Kaspersky Security Center policies.

The following settings are reset or set to default values for the new version of the application after upgrading of the application and its plug-ins to version 5.0:

- All counters, including anti-virus database statuses
- Data about installed updates of application modules and anti-virus databases
- Task statuses
- User access permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service
- Application and task settings configured through the registry
- Application and task settings that were changed during the installation of critical fixes
- Event configuration
- Settings of data transfer to the Kaspersky Security Center Administration Server: by default, the transfer of all data is enabled
- Trace and dump settings
- Settings of the application's local tasks located on the **Notifications** tab

Settings that did not exist in the version of the application that you are updating get default values.

Limitations of settings and components migration

- The contents of the Quarantine of the version being upgraded is moved to the Backup of version 5.0. After the upgrade, the maximum size of Backup is set to the sum of the maximum sizes of the Backup and Quarantine of the application being upgraded; the available space threshold is updated accordingly. At the same time, the default maximum size of Backup is increased to 400 MB, and the available space threshold is increased to 100 MB.

- Kaspersky Industrial CyberSecurity for Nodes 4.0 settings **Quarantine folder**, **Backup folder**, and **Folder for restoring objects** do not exist in Kaspersky Industrial CyberSecurity for Nodes 4.5 and later, therefore they are not migrated. Other settings that exist in the old version, but not in the new version are likewise not migrated.

- When migrating the [KICS+KEA] configuration to [KICS+built-in agent], the contents of the Kaspersky Endpoint Agent Quarantine is migrated to the Kaspersky Industrial CyberSecurity for Nodes 5.0 Quarantine.

- The list of blocked network sessions of client computers is not migrated. At the same time, the settings for automatically unblocking access to blocked network file resources remain unchanged after the application upgrade.

- Password protection settings are not migrated. In Kaspersky Industrial CyberSecurity for Nodes 4.5, Password protection underwent significant changes. If necessary, turn on Password protection and set a password.

- Trusted zone:

  - The method of selecting trusted zone objects has been changed in Kaspersky Industrial CyberSecurity for Nodes 5.0. Exclusions defined as individual files or file or folder paths can be migrated. Exclusions defined as a predefined scope (for example, hard drives) or a script URL are not migrated. After migration, you must add such exclusions manually.

  - Predefined scan exclusions and trusted applications that help set up the application on servers and its interaction with industrial software have been added to the trusted zone.

- The Applications Launch Control and Device Control components have been significantly reworked. Component settings of the version being upgraded are migrated with consideration of the new settings structure in Kaspersky Industrial CyberSecurity for Nodes 5.0. This means that you may need more space on the Administration Server to store application settings.

- Settings of the File Integrity Monitor and Registry Access Monitoring components of the application version being upgraded are migrated to the settings of the System Integrity Monitoring component.

- The Firewall Management component has been reworked into the Firewall component, which, in addition to interfacing with the Windows firewall, now additionally functions as a firewall. After completing the migration, you must configure the component mode from scratch.

- To use KSN, you must read and accept the KSN Statement again.

- Versions 4.5 and later of the application do not support scheduling individual components. If the components are enabled, they keep running while the application is running.

- When migrating tasks, the scheduled start time for the task is offset by the number of hours that matches the number of the timezone configured in the OS settings of the computer on which the migration is being performed. For example, suppose the start time of the task in the earlier version of the application is 7:00, and the time zone configured for the operating system is UTC +3:00. Then, after the task is migrated, the start time changes to 10:00.

- The section for setting up the actions to perform on probably infected objects has been removed from the settings of the Real-Time File Protection component and On-Demand Scan tasks. These settings are not migrated to the newer application version.

- If you are using version 4.5 or later of the application as part of the Kaspersky Industrial CyberSecurity Endpoint Detection and Response solution, to manage alert details, you must upgrade the web plug-in of Endpoint Detection and Response to version 15.1 or later. Otherwise, if you have the Kaspersky Endpoint Agent web plug-in installed, threat development chains in incident cards opened with this web plug-in may contain limited data or errors.

- Kaspersky Security Center Web Console or Administration Console cannot be used to send Quarantine and Backup objects to Kaspersky for analysis if they were migrated after upgrading version 4.0 or earlier of the application to 4.5 or later, or if the objects were placed in storages by Kaspersky Anti Targeted Attack Platform or Kaspersky Industrial CyberSecurity for Networks scenarios.

- When migrating On-Demand Scan tasks, the default security level for predefined scan scopes changes from *Inform* to *Custom*.

- Events sent to SIEM now use a new date and time format. In previous versions of Kaspersky Industrial CyberSecurity for Nodes, events were generated with a timestamp. Now the application generates events with the date and time in the `<DATE-TIME>` format. If necessary, reconfigure the SIEM interaction to have the date and time converted to the timestamp format.

- If a component that was previously included in the installation is not installed during a local upgrade of Kaspersky Industrial CyberSecurity for Nodes, settings of such a component are not preserved. If you subsequently install this component, default settings will be applied to it.

Correspondence of components and tasks in Kaspersky Industrial CyberSecurity for Nodes versions 4.0 and 5.0

When upgrading Kaspersky Industrial CyberSecurity for Nodes 4.0 to version 5.0, the set of components and tasks is migrated only if the application is installed locally.

Correspondence of components in Kaspersky Industrial CyberSecurity for Nodes versions 4.0 and 5.0

Component of Kaspersky Industrial CyberSecurity for Nodes 4.0	Component of Kaspersky Industrial CyberSecurity for Nodes 5.0
Trusted zone	Trusted zone
Real-Time File Protection	Real-Time File Protection
KSN Usage	KSN Usage
Exploit Prevention	Exploit Prevention
Network Threat Protection	Network Threat Protection
AMSI Scanner	AMSI Scanner
Applications Launch Control	Applications Launch Control
Device Control	Device Control
Wi-Fi Control	Device Control The functionality of the Wi-Fi Control component has been merged into the Device Control component.
Firewall Management	Firewall The Windows Firewall acts as the firewall of Kaspersky Industrial CyberSecurity for Nodes 4.0, while the application manages the Windows Firewall. In Kaspersky Industrial CyberSecurity for Nodes 5.0, a separate component is responsible for the Firewall functionality.

Component of Kaspersky Industrial CyberSecurity for Nodes 4.0	Component of Kaspersky Industrial CyberSecurity for Nodes 5.0
Anti-Cryptor	Anti-Cryptor
File Integrity Monitor	System Integrity Monitoring The functionality of the File Integrity Monitor and Registry Access Monitoring components has been merged into the System Integrity Monitoring component.
Log Inspection	Log Inspection
Registry Access Monitoring	System Integrity Monitoring The functionality of the File Integrity Monitor and Registry Access Monitoring components has been merged into the System Integrity Monitoring component.
Portable scanner	Portable Auditor
(none)	Remediation Engine
(none)	Integration with KICS for Networks Component acting as the Kaspersky Endpoint Agent.
(none)	SIEM Integration Component acting as the Kaspersky Endpoint Agent.
(none)	Managed Detection and Response (Industrial CyberSecurity) Component acting as the Kaspersky Endpoint Agent.
(none)	Endpoint Detection and Response Expert (on-premises) Component acting as the Kaspersky Endpoint Agent.
(none)	Endpoint Detection and Response (Industrial CyberSecurity)
(none)	Anomaly Detection using Sigma rules Component acting as the Kaspersky Endpoint Agent.
Task of Kaspersky Industrial CyberSecurity for Nodes 4.0	**Task of Kaspersky Industrial CyberSecurity for Nodes 5.0**
Activating the application	Application activation
Copying Updates	Update The functionality of the Copying Updates task has been merged into the Update task.
Baseline File Integrity Monitor	Baseline System Integrity Monitor
Database Update	Update The functionality of the Database Update task has been merged into the Update task.
Software Modules Update	Update The functionality of the Software Modules Update task has been merged into the Update task.
Rollback of Application Database Update	Update rollback
On-Demand Scan	On-Demand Scan
Application Integrity Control	Application Integrity Control
Rule Generator for Applications Launch Control	Rule Generator for Applications Launch Control
Rule Generator for Device Control	Rule Generator for Device Control
(none)	Administration Server connection protection
(none)	Change Kaspersky Industrial CyberSecurity for Nodes components
(none)	Security Audit Task implementing Kaspersky Endpoint Agent functionality.
(none)	Terminate process Task implementing Kaspersky Endpoint Agent functionality.

Component of Kaspersky Industrial CyberSecurity for Nodes 4.0	Component of Kaspersky Industrial CyberSecurity for Nodes 5.0
(none)	Start process Task implementing Kaspersky Endpoint Agent functionality.
(none)	IOC Scan Task implementing Kaspersky Endpoint Agent functionality.
(none)	Get file Task implementing Kaspersky Endpoint Agent functionality.
(none)	Move file to Quarantine Task implementing Kaspersky Endpoint Agent functionality.
(none)	Delete file Task implementing Kaspersky Endpoint Agent functionality.

Installing and removing Kaspersky Security Gateway

This section provides instructions for installing and removing Kaspersky Security Gateway.

Updating Kaspersky Security Gateway

The Kaspersky Security Gateway update is performed by installing the new version over the installed version of the application and does not require a restart.

When upgrading Kaspersky Security Gateway to version 5.0, the previously installed version of the application is automatically deleted.

The settings values of the previously installed Kaspersky Security Gateway version are transmitted unchanged to Kaspersky Security Gateway 5.0.

Updating Kaspersky Security Gateway from version 4.5 or earlier to 5.0 disables trace file logging. If necessary, configure trace file logging again.

Installing Kaspersky Security Gateway using the Setup Wizard

To install Kaspersky Security Gateway,

run the security_gateway.msi file included in the distribution kit.

The corresponding wizard will guide you through the installation. Follow the instructions of the Wizard.

The interface of the Kaspersky Security Gateway Setup Wizard consists of a sequence of windows (steps). To move between windows of the Setup Wizard, use the **< Back** and **Next >** buttons. To close the Setup Wizard when you are done, click the **Finish** button. To exit the Setup Wizard at any stage of the installation process, click the **Cancel** button.

Step 1. Verifying installation requirements

If there is an older version of Kaspersky Security Gateway among the detected applications, the Setup Wizard automatically removes the old version and installs the new version of Kaspersky Security Gateway.

If there is Kaspersky Security Gateway 2.0 or an earlier version installed, the Setup Wizard will not remove the old version and will cancel the installation. Before installing Kaspersky Security Gateway 5.0, manually remove Kaspersky Security Gateway 2.0 or any earlier version.

Before installing or upgrading Kaspersky Security Gateway, the Setup Wizard verifies that the following requirements are satisfied:

- The computer and installed software meet the hardware and software requirements.
- The user account has the privileges needed to install applications.

If any one of the previous requirements is not met, a relevant notification is displayed on the screen, and the installation process is aborted.

Step 2. Welcome page of the installation procedure

If the computer on which you are installing Kaspersky Security Gateway fully meets the hardware and software requirements, the welcome page of the installation process opens. The welcome page announces the beginning of installation of Kaspersky Security Gateway on the computer.

Proceed to the next step of the Wizard.

Step 3. Viewing the End User License Agreement and Privacy Policy

At this step, you must read the Kaspersky End User License Agreement and Privacy Policy.

If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select the **I accept the terms of the End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes.

If you do not accept the End User License Agreement and/or Privacy Policy the installation will be aborted.

Proceed to the next step of the Wizard.

Step 4. Selecting the destination folder

At this step, you have to specify the path to the destination folder where Kaspersky Security Gateway will be installed. To select the destination folder, click the **Browse** button.

Proceed to the next step of the Wizard.

Step 5. Selecting components

At this step, you can select the Kaspersky Security Gateway components that you want to install. All components are selected for installation by default.

To select a component that you want to install, click the icon next to the component name to bring up the context menu. Then select **Feature will be installed on the local hard drive** or **Entire feature and its subfeatures will be installed on local hard drive**. For more details on what tasks are performed by the selected component and how much disk space is required to install the component, refer to the lower part of the current Setup Wizard page.

To view detailed information about the available space on local hard drives, click the **Volume** button. Information is shown in the **Disk Space Requirements** window that opens.

To cancel component installation, in the context menu, select the **Feature will be unavailable** option.

To return to the list of components installed by default, click the **Reset** button.

Proceed to the next step of the Wizard.

Step 6. Configuring the connection to the SCADA system

At this step, you need to specify SCADA connection settings:

- For an IEC 60870-5-104 connection: the address (a number from 1 to 65535) and TCP port (a number from 1 to 65535) of the computer on which Kaspersky Security Gateway will be installed.
- For an OPC UA connection: the TCP port (a number from 1 to 65535) of the computer on which Kaspersky Security Gateway will be installed.

To install the program, click the **Install** button.

Current network connections may be terminated while Kaspersky Security Gateway is being installed on the computer. Most terminated connections are restored after a short time.

Step 7. Installing Kaspersky Security Gateway

The Setup Wizard copies Kaspersky Security Gateway files to the computer. Wait for the installation to complete.

Finish the wizard.

Installing Kaspersky Security Gateway from the command line

To install Kaspersky Security Gateway from the command line, run the following command:

```
msiexec /i security_gateway.msi EULA=1 PRIVACYPOLICY=1 /qn
```

where `EULA=1 PRIVACYPOLICY=1` – accept the terms of the Kaspersky Security Gateway End User License Agreement between you and Kaspersky and the Privacy Policy that describes processing and transmission of data.

By setting parameters to 1, you confirm the following:

- You have fully read, understood and accept the terms and conditions of End-User License Agreement.
- You have fully read and understood the Privacy Policy, you are aware and agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy.

You must accept the terms of the End-User License Agreement and the Privacy Policy to install Kaspersky Security Gateway.

The text of the End-User License Agreement and Privacy Policy is included in the distribution kit.

Removing Kaspersky Security Gateway

Administrator account permissions are required for removing Kaspersky Security Gateway.

To remove Kaspersky Security Gateway:

1. Open the Microsoft Windows Control Panel.
2. On the Microsoft Windows Control Panel, click the **Programs and Features** icon.

   The **Uninstall or change a program** window opens in Microsoft Windows.
3. In the **Uninstall or change a program** window, select **Kaspersky Security Gateway** and click the **Change** button.

   The Setup Wizard starts.
4. In the **Modify, Repair, or Remove application** window of the Setup Wizard, click the **Remove** button.

The Setup Wizard prompts you to configure the removal settings. Follow the instructions of the Wizard.

Step 1. Saving Kaspersky Security Gateway data for future use

At this step, the Setup Wizard prompts you to save Kaspersky Security Gateway configuration file for future use during subsequent installation of Kaspersky Security Gateway (for example, when installing a new version).

To save Kaspersky Security Gateway configuration file,

select the **Save application configuration file** check box.

The **Save application configuration file** option is only available if the Setup Wizard is run by clicking the **Change** button in the **Programs and Features** section of the Control Panel.

Proceed to the next step of the Wizard.

Step 2. Removing Kaspersky Security Gateway

At this step, the Setup Wizard removes Kaspersky Security Gateway from the computer. Wait until the removal process is complete.

Finish the wizard.

When removing Kaspersky Security Gateway, your operating system may require a restart. If you decide to not restart immediately, the Kaspersky Security Gateway removal will not finish until the operating system is restarted, or until the computer is turned off and then turned on again.

Installing OPC Core Components Redistributables

Starting from Kaspersky Industrial CyberSecurity for Nodes version 5.0, the OPC Core Components Redistributables package is not included in the Kaspersky Security Gateway installation package.

If you plan to use the OPC DA protocol for data transfer, when installing Kaspersky Security Gateway 5.0 or later, or upgrading the application, you need to install the OPC Core Components Redistributables package on your own if this package has not been installed by another application. You can use the opc_redist.msi file included in distribution kit.

If you installed OPC Core Components Redistributables after installing Kaspersky Security Gateway, you need to restart the Kaspersky Security Gateway OPC service.

Application interface

You can control Kaspersky Industrial CyberSecurity for Nodes using the following interfaces:

- Application Console.
- Kaspersky Security Center Administration Console.
- Kaspersky Security Center Web Console.

Kaspersky Security Center Administration Console

Kaspersky Security Center lets you remotely install and uninstall, start and stop Kaspersky Industrial CyberSecurity for Nodes, configure application settings, change the set of available application components, add keys, and start and stop tasks.

The application can be managed via Kaspersky Security Center using the Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in. See detailed information about the Kaspersky Security Center interface in the Kaspersky Security Center Help.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (hereinafter also referred to as Web Console) is a web application intended for centrally performing the main tasks to manage and maintain the security system of an organization's network. Kaspersky Security Center Web Console – is a Kaspersky Security Center component that provides a user interface. For detailed information about Kaspersky Security Center Web Console, please refer to the Kaspersky Security Center Help.

The following actions are available for Web Console:

- Monitor the status of your organization's security system.
- Install Kaspersky applications on devices within your network.
- Manage installed applications.
- View reports on the security system status.

Working with the Administration Plug-in

This section provides information about the Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in and describes how to manage the application installed on a protected device or on a group of protected devices.

Managing Kaspersky Industrial CyberSecurity for Nodes from Kaspersky Security Center

You can centrally manage several protected devices that have Kaspersky Industrial CyberSecurity for Nodes installed and are joined to the same administration group via the Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in. Kaspersky Security Center also lets you separately configure the settings of each protected device included in the administration group.

An administration group is created manually via Kaspersky Security Center. The group includes several devices with Kaspersky Industrial CyberSecurity for Nodes installed for which you want to configure the same control and protection settings. For details on using administration groups, see Kaspersky Security Center Help.

Application settings for a single protected device are unavailable if the operation of Kaspersky Industrial CyberSecurity for Nodes on the protected device is controlled by an active Kaspersky Security Center policy.

No additional actions are required to start the Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in in Kaspersky Security Center. Once the Management Plug-in is installed on the administrator's protected device, it is started together with any type of the Kaspersky Security Center Administration Console.

Kaspersky Industrial CyberSecurity for Nodes can be managed from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of devices. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the **Properties: <Protected device name>** window of Kaspersky Security Center.

  Policies can be used to configure general application settings, settings for real-time computer protection tasks, activity control tasks on devices, network storage protection tasks and settings for starting local system tasks on a schedule.

- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of devices.

  You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for protected devices that do not belong to any administration group.

- **Using the properties window of a single device**. In the **Properties: <Protected device name>** window, you can remotely configure the task settings for an individual protected device included in an administration group. You can also configure both general application settings and settings for all Kaspersky Industrial CyberSecurity for Nodes tasks if the selected protected device is not controlled by an active Kaspersky Security Center policy.

Managing application settings

This section contains information about configuring Kaspersky Industrial CyberSecurity for Nodes general settings in the Kaspersky Security Center Administration Console.

Configuring general application settings in Kaspersky Security Center

You can configure Kaspersky Industrial CyberSecurity for Nodes general settings from Kaspersky Security Center for a group of protected devices or for one protected device.

Configuring interface and scan settings in Kaspersky Security Center

To configure scalability settings and the application interface:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Application settings** section, click the **Settings** button in the **Interface settings** subsection.

5. In the **Interface settings** window, on the **General** tab, configure the following settings:

   - In the **Interaction with user** section configure whether the System Tray Icon will be displayed in the taskbar after each application start.

     - **Display user interface**. On the client computer, an icon is available in the Windows tray. In the context menu of the icon, the user can perform operations with Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes also displays notifications above the application icon. The context menu of the icon in the Windows system tray lets you open the Compact Diagnostic Interface. Clicking a link in the Compact Diagnostic Interface opens the Application Console.

     - **Do not display user interface**. On a client computer, no signs of Kaspersky Industrial CyberSecurity for Nodes operation are displayed. The icon in the Windows notification area and notifications are not available.

   - In the **Statuses** section, you can specify which warnings you want to see on the Kaspersky Industrial CyberSecurity for Nodes system tray icon.

6. Click **OK**.

The configured application settings are saved.

Configuring security settings in Kaspersky Security Center

To configure security settings manually:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Application settings** section, click the **Settings** button in the **Security and reliability** subsection.

5. In the **Security settings** window, on the **Security** tab, configure the following settings:

   - In the **General** section, we recommend leaving the **Start the application on computer startup (recommended)** enabled (default).

   - In the **Self-Defense** section, enable or disable the **Protect application processes from external threats** functionality.

   - In the **Actions when switching to UPS backup power** section, specify limitations on protected device load created by Kaspersky Industrial CyberSecurity for Nodes after switching to UPS power:

     - **Do not start scheduled scan tasks**

     - **Stop running scan tasks**

- In the **Computer status when settings are applied** section, configure the display of the status of client computers with the application installed if errors occur when applying a policy or running a task.

- In the **Compatibility settings** section, configure the **Compatibility with remote administration software** setting.

6. On the **Scan settings** tab, configure the following settings:

   - **Limit CPU usage for scan tasks**. Kaspersky Industrial CyberSecurity for Nodes limits its use of the protected device CPU during on-demand scan tasks to the value specified in the **Upper limit** field. Enabling of this option can negatively affect the performance of Kaspersky Industrial CyberSecurity for Nodes.

   - **Yield resources to other applications**. Consumption of computer resources by Kaspersky Industrial CyberSecurity for Nodes when scanning the computer may increase the load on the CPU and hard drive subsystems. This may slow down other applications. To optimize the performance, Kaspersky Industrial CyberSecurity for Nodes provides a mode for transferring resources to other applications. In this mode, the operating system can decrease the priority of Kaspersky Industrial CyberSecurity for Nodes scan task threads when the CPU load is high. This allows redistributing operating system resources to other applications. Thus, scan tasks will receive less CPU time. As a result, Kaspersky Industrial CyberSecurity for Nodes will take longer to scan the computer. By default, the application is configured to concede resources to other applications.

7. Click **OK**.

The scalability and reliability settings are saved.

Configuring connection settings using Kaspersky Security Center

The configured connection settings are used to connect Kaspersky Industrial CyberSecurity for Nodes to update and activation servers and during integration of applications with Kaspersky Security Network services.

To configure the connection settings take the following steps:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Application settings** section, click the **Settings** button in the **Connection settings** subsection.

   The **Connection settings** window opens.

5. In the **Proxy server** section, click **Settings**.

6. This opens a window; in that window, in the **Proxy server settings** section, select an option for managing proxy settings:

   - **Do not use a proxy server**. If this option is selected, Kaspersky Industrial CyberSecurity for Nodes does not use a proxy server.
   - **Automatically detect proxy server settings.** If this option is selected, Kaspersky Industrial CyberSecurity for Nodes uses proxy settings of the operating system.
   - **Use specified proxy server settings**. If this option is selected, Kaspersky Industrial CyberSecurity for Nodes uses proxy server settings specified manually. Enter the IP address or symbolic name of the proxy server and the port number

     If necessary, clear the **Bypass a proxy server for local addresses** check box. If this functionality is enabled, devices are accessed directly from the network that hosts the protected device with Kaspersky Industrial CyberSecurity for Nodes installed. This option is enabled by default.

7. In the **Proxy server authentication settings** section, in the drop-down list, select the method for authenticating at the proxy server:

   a. If you selected **Automatically detect proxy server settings**:

      - **Do not use authentication**.
      - **NTLM authentication**. NTLM authentication with the current user account (default).
      - **Kerberos authentication**. Kerberos authentication with the current user account.

   b. If you selected **Use specified proxy server settings**:

      - **Do not use authentication**.
      - **NTLM authentication**. NTLM authentication with the current user account (default).
      - **NTLM authentication with user name and password**. NTLM authentication with manually specified credentials.
      - **Kerberos authentication**. Kerberos authentication with the current user account.

        To ensure the Kerberos authentication works correctly when using CNAME records for the proxy server address, you must register a Service Principal Name (SPN) for each CNAME record.

      - **Kerberos authentication with user name and password**. Kerberos authentication with manually specified credentials.
      - **User name and password**. Authentication with manually specified credentials.

     If necessary, enter a user name and a password.

     If Kerberos authentication is selected, Kaspersky Industrial CyberSecurity for Nodes can, depending on the proxy server settings, perform authentication using either the Kerberos or NTLM protocol.

8. In the **Licensing** section, select or clear the **Use Kaspersky Security Center as a proxy server when activating the application** check box.

9. Click **OK**.

10. In the **Monitored ports** section, specify an option for network port:

    - **Monitor all network ports**. In this network port monitoring mode the protection components monitor data streams that are transmitted via any open network ports of the computer.

    - **Monitor selected network ports only**. In this network port monitoring mode, the protection components monitor the selected ports of the computer and the network activity of the selected applications. The list of network ports that are normally used for transmission of email and network traffic is configured according to the recommendations of Kaspersky experts. If necessary you can edit the list of network ports.

11. Click the **Settings** button and edit the following settings:

    - **Monitor all ports for the applications from the list recommended by Kaspersky**. Kaspersky Industrial CyberSecurity for Nodes monitors network ports of applications from the predefined list. For example, this list includes Google Chrome, Adobe Reader, Java, and other applications.

    - **Monitor all ports for specified applications**. Kaspersky Industrial CyberSecurity for Nodes monitors network ports of applications added to the list.

12. Click **OK**.

    The configured connection settings are saved.

Configuring the local task run mode

You can use policies to allow or block the start of the local system On-Demand Scan task and the Update task. This is done according to the schedule configured locally on each protected device in the administration group:

- If the scheduled start of a specific type of local system task is prohibited by a policy, these tasks will not be performed on the protected device according to the schedule. You can start local system tasks manually.

- If the scheduled start of a specific type of local system task is allowed by a policy, these tasks will be performed in accordance with the scheduled parameters configured locally for this task.

By default, starting of local system tasks is prohibited by policy.

> We recommend that you do not allow local system tasks to start if updates or on-demand scans are administered by Kaspersky Security Center group tasks.

If you do not use group update or on-demand scan tasks, allow local system tasks to be started in the policy: Kaspersky Industrial CyberSecurity for Nodes will perform application database and module updates, and start all local system on-demand scan tasks in accordance with the default schedule.

You can use policies to allow or block the scheduled start of the following local system tasks:

- On-Demand Scan tasks: *Critical Areas Scan*, *Scan at Operating System Startup*, *Application Integrity Control*, *Baseline System Integrity Monitor*.
- Update tasks: *Update of databases and application modules*, *Application update*.

If the protected device is excluded from the administration group, the local system tasks schedule will be enabled automatically.

To allow or block startup schedule management for the application local tasks in a policy:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node, expand the relevant group, and in the results pane, select the **Policies** tab.
2. On the **Policies** tab, in the context menu of the policy for which you want to schedule Kaspersky Industrial CyberSecurity for Nodes local system tasks for the group of protected devices, select **Properties**.
3. In the policy properties window, select the **Application settings** section.
4. Click **Settings** in the **Run local system tasks** subsection.
5. Select the **Allow use of local tasks** check box.
6. Use the **Allow schedule management** check box to allow or block startup schedule management for the application local tasks.

Configuring Quarantine and Backup settings in Kaspersky Security Center

To configure general Quarantine and Backup settings in Kaspersky Security Center:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. Go to the **Supplementary** section.
5. Click the **Settings** button in the **Storages** subsection.
6. Configure the settings described in the table below.

Storage settings

Parameter	Description
On the **Reports** tab, specify the reports settings:	
Store reports no longer than	If the check box is selected, the maximum report storage term is limited to the defined time interval. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file.
Limit the size of report file to	If the check box is selected, the maximum report file size is limited to the defined value. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file when the maximum report file size is reached.
On the **Backup** tab, specify the Backup settings:	
Store objects no longer than	If the check box is selected, the maximum file storage term is limited to the defined time interval. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Industrial CyberSecurity for Nodes deletes the oldest files from Backup.
Limit the size of Backup to	If the check box is selected, the maximum storage size is limited to the defined value. By default, the maximum size is 400 MB. To avoid exceeding the maximum storage size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest files from storage when the maximum storage size is reached.
Threshold value for available space	The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value is 100 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the amount of free space in Backup. The **Threshold value for available space** check box is active if the **Limit the size of Backup to** check box is selected.
On the **Quarantine** tab, specify the Quarantine settings:	
Limit the size of Quarantine to	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes monitors the total size of objects placed in Quarantine. If the specified value is exceeded (the default value is 1024 MB), Kaspersky Industrial CyberSecurity for Nodes logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type. Meanwhile the application stops quarantining new objects. You must empty the Quarantine manually. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the total size of objects placed in Quarantine. By default, the functionality is disabled.
Threshold value for available space	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the minimum amount of free space in Backup (the default value is 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Quarantine free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. The **Threshold value for available space** check box is active if the **Limit the size of Quarantine to** check box is selected. This option is enabled by default.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Industrial CyberSecurity for Nodes on several protected devices.

Global Kaspersky Security Center policies can be created for managing protection on several devices where Kaspersky Industrial CyberSecurity for Nodes is installed.

A policy enforces the Kaspersky Industrial CyberSecurity for Nodes settings, functions and specified tasks on all the protected devices for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has *Active* status in the Administration Console.

Information on policy enforcement is logged in the Kaspersky Industrial CyberSecurity for Nodes system audit log. This information can be viewed in the Application Console in the **Log Inspection** node.

Kaspersky Security Center offers one way to apply policies on protected devices: *Prohibit editing of settings*. After a policy has been applied, Kaspersky Industrial CyberSecurity for Nodes uses the values of settings for which you have specified in the policy properties that **Editing prohibited** . In this case, Kaspersky Industrial CyberSecurity for Nodes does not use the values of settings in effect before the policy was applied. Kaspersky Industrial CyberSecurity for Nodes does not apply the values of active policy settings for which you have specified in the policy properties that **Editing allowed** .

If a policy is active, the values of settings marked with the icon in the policy are displayed in the Application Console but cannot be edited. The values of other settings can be edited in the Application Console.

The settings configured in the active policy and marked with the icon also block changes in Kaspersky Security Center for an individual protected device in the **Properties: <Protected device name>** window.

Settings that are specified and sent to the protected device using an active policy are saved in the local task settings after the active policy is disabled.

If a policy defines the settings of a currently running Real-Time Computer Protection task or Network-Attached Storages Protection task, the settings defined by the policy will change immediately after the policy is applied. If the task is not running, the settings are applied when it starts.

Creating a policy

Before creating a policy, you need to install the Administration Plug-in klcfginst.exe.

To create a policy for a group of protected devices where application is installed and running:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree, then select the administration group containing the protected devices for which you wish to create a policy.
2. In the results pane of the selected administration group, select the **Policies** tab and click the **New policy** button to start the New Policy Wizard.

   The **New policy wizard** window opens.
3. In the **Select the application for which you want to create a group policy** window, select Kaspersky Industrial CyberSecurity for Nodes.
4. Click **Next**.
5. Enter a group policy name in the **Name** field.

   The policy name cannot contain the following symbols: `" * < : > ? \ |` .
6. To apply a policy configuration used in a previous version of the application:

   a. Select the **Use policy settings for an earlier version of the application** check box.

   b. Click **Browse**.

c. Select the policy you want to apply.

d. Click **Next**.

7. In the **Operation type selection** window, in the **Configure Real-Time File Protection** block, select the **Enable Real-Time File Protection** check box and specify the security level.

   If the task run mode is not selected, you cannot proceed to the next step of the New Policy Wizard.

8. Configure Real-Time Computer Protection.

9. Configure scan exclusions and trusted applications.

10. Select one of the following policy statuses in the **Create the group policy for the application** window:

    - **Active policy**, if you want to apply the policy immediately after it is created. If an active policy already exists in the group, it is deactivated and a new policy is applied.
    - **Inactive policy**, if you do not want to apply the created policy immediately. In this case the policy may be activated later.
    - **Out-of-office policy**, the policy is activated when a computer leaves the organization network perimeter.
    - Select the **Open policy properties immediately after it is created** check box to automatically close the **New policy wizard** and configure the newly created policy after clicking the **Next** button.

11. Click **Finish**.

    The created policy appears in the list of policies on the **Policies** tab of the selected administration group. In the **Properties: <Policy name>** window, you can configure other settings, tasks and functions of Kaspersky Industrial CyberSecurity for Nodes.

After a new policy is created, a set of allowing rules is created to prevent applications from being blocked, ensuring their uninterrupted operation.

By default, Kaspersky Industrial CyberSecurity for Nodes creates a set of rules for inbound network traffic when creating a new policy:

- Two allowing rules for the process of sharing the Windows desktop using Kaspersky Security Center Network Agent, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 15000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

By default, Kaspersky Industrial CyberSecurity for Nodes creates a set of outgoing network traffic rules when creating a new policy:

- Two allowing rules for the Kaspersky Industrial CyberSecurity for Nodes service, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for the worker process of Kaspersky Industrial CyberSecurity for Nodes, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 13000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

Configuring a policy

To configure the policy settings:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Expand the administration group for which you want to configure the associated policy settings, and open the **Policies** tab in the details pane.
3. Click the policy name you want to configure.

   Open the **Properties: <Policy name>** window in one of the following ways:

   - Selecting the **Properties** option in the policy context menu.
   - Double-clicking the selected policy.
4. On the **General** tab in the **Policy status** section, enable or disable the policy. To do so, select one of the options below:

   - **Active policy**, if you want the policy to be applied on all protected devices within the selected administration group.
   - **Out-of-office policy**, the policy is activated when a computer leaves the organization network perimeter.
   - **Inactive policy**, if you want to activate the policy later on all protected devices within the selected administration group.
5. Configure application settings in the other sections of the policy.

   You can enable or disable the execution of any task on all protected devices within the administration group by means of a Kaspersky Security Center policy.

You can configure the application of policy settings on all network protected devices for each individual software component.

6. Click **OK**.

The configured settings are applied in the policy.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Industrial CyberSecurity for Nodes tasks, and how to create them, configure task settings, and start and stop them.

About task creation in Kaspersky Security Center

You can create group tasks for administration groups and sets of protected devices. You can create the following types of tasks via Kaspersky Security Center:

- *Application Activation*
- *Security Audit*
- *Terminate process*
- *Run process*
- *Administration Server connection protection*
- *Change Kaspersky Industrial CyberSecurity for Nodes components*
- *Baseline System Integrity Monitor*
- *Update*
- *Update rollback*
- *IOC Scan*
- *Get file*
- *Move file to Quarantine*
- *On-Demand Scan*
- *Application Integrity Control*
- *Remove key*

- *Delete file*
- *Rule Generator for Applications Launch Control*
- *Rule Generator for Device Control*.

You can create local and group tasks in the following ways:

- For an individual protected device in the **Tasks** section.
- For an administration group: in the details pane of the node of the selected group of protected devices on the **Tasks** tab.
- For a set of protected devices: in the details pane of the **Device selections** node.

You can use policies to disable schedules for *Update* and *On-Demand Scan* local system tasks on all protected devices in the same administration group.

General information on tasks in Kaspersky Security Center is provided in the Kaspersky Security Center Help.

Creating a task using Kaspersky Security Center

To create a new task in the Kaspersky Security Center Administration Console:

1. Start the task wizard in one of the following ways:
   - To create a local task:
     a. Expand the **Managed devices** node in the Administration Console tree and select the group that the protected server belongs to.
     b. In the results pane of the **Devices** tab, open the context menu of the protected device and select **Properties**.
     c. In the window that opens, in the **Tasks** section, click the **Add** button.
   - To create a group task:
     a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
     b. Select the administration group for which you want to create a task.
     c. In the results pane, open the **Tasks** tab and select **New task**.

   The task wizard window opens.
2. In the **Select the task type** window, under the heading **Kaspersky Industrial CyberSecurity for Nodes**, select the type of the task to be created.

3. Depending on the task type, the settings may vary:

   - Create an On-Demand Scan task.
   - To create an update task, configure task settings based on your requirements:

     a. You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source in the **Update source** block. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.

        You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

     b. Configure the settings for a feature that reduces the load on the disk subsystem:

     c. You can specify the actions that Kaspersky Industrial CyberSecurity for Nodes will perform if critical application module updates are needed, as well as after installation of critical updates is complete. In addition, you can specify whether Kaspersky Industrial CyberSecurity for Nodes will receive information about available scheduled updates.

     d. Specify the set of updates to copy and a path to the folder that will be used by Kaspersky Industrial CyberSecurity for Nodes to store copied updates.

   - To create the *Application Activation* task:

     a. In the **Activation settings** window, specify the key file or activation code that you want to use to activate the application.

     b. Select the **Use as additional key** check box if you want to create a task for renewing the license.

   - Create the Rule Generator for Applications Launch Control task.
   - Create the Rule Generator for Device Control task.

4. Configure the task schedule.

5. Click **OK**.

6. If the task is being created for a set of protected devices, select the network (or group) of protected devices on which this task will be executed.

7. In the **Selecting an account to run the task** window, specify the account you want to use to run the task.

8. In the **Define the task name** window, enter the task name (no longer than 100 characters, not containing the symbols `" * < > ? \ | :`).

   We recommend that you add the task type to the task name (for example, "On-demand scan of shared folders").

9. In the **Finish task creation** window, do the following:

   a. Select the **Run the task after the wizard finishes** check box if you want the task to start as soon as it is created.

   b. Click **Finish**.

The created task is displayed in the **Tasks** list.

Going to the local task settings and general application settings for an individual computer

If the application is currently under the Kaspersky Security Center policy and this policy prohibits changing the application settings, you cannot edit these settings for an individual computer.

To go to the local task settings for an individual computer:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected device belongs to.
3. In the results pane, select the **Devices** tab.
4. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - in the context menu of the name of the protected device, select **Properties**.

   The **Properties: <Protected device name>** window opens.
5. Go to the **Tasks** section.
6. In the task list, select a local task to configure in one of the following ways:
   - double-click on the task name
   - select a task in the list and click the **Properties** button
   - in the context menu on the task name, select **Properties**.

   The **Properties: <Task name>** window opens.

To go to the general application settings for an individual computer:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the group that the protected device belongs to.
2. In the results pane, select the **Devices** tab.
3. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - in the context menu of the name of the protected device, select **Properties**.

   The **Properties: <Protected device name>** window opens.
4. Go to the **Applications** section.

5. In the list of installed applications, select Kaspersky Industrial CyberSecurity for Nodes in one of the following ways:

   - double-click the name of Kaspersky Industrial CyberSecurity for Nodes
   - select Kaspersky Industrial CyberSecurity for Nodes in the list and click the **Properties** button.
   - in the context menu of the name of Kaspersky Industrial CyberSecurity for Nodes, select the **Properties** item.

   The **Settings** window of **Kaspersky Industrial CyberSecurity for Nodes** opens.

Configuring group tasks in Kaspersky Security Center

To configure a group task for multiple protected devices:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:

   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

5. In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
6. Depending on the type of configured task, do one of the following:

   - To configure the *On-Demand Scan* task:
     - In the **Scan scope** section, configure a scan scope.
     - In the **Settings** section, configure the task priority level and integration with other software components.
   - To configure the *Update* task:
     - Go to the **Settings** section and specify the **Application databases and modules update settings**.
     - Choose an action to perform: copy and install critical updates of software modules or only check for them.

- To configure the *Application Activation* task:
  - In the **Settings** section, specify the key file or activation code that you want to use to activate the application.
  - Select the **Use as additional key** check box if you want to add an activation code or key file for renewing the license.
- To configure the *Rule Generator for Device Control* task, in the **Settings** section, specify the settings that you want to use to create the list of Device Control rules.

7. Configure the task schedule in the **Schedule** section.
8. In the **Account** section, specify the account whose rights will be used to run the task. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
9. If necessary, in the **Exclusions from task scope** section, specify objects that you want to exclude from the scope of the task. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
10. Click the **OK** button in the **Properties: <Task name>** window.

The newly configured group task settings are saved.

Configurable settings of group tasks are listed below.

- Rule Generator for Applications Launch Control

  While configuring the *Rule Generator for Applications Launch Control* task settings, you can select how you want to create allowing rules on the **Rules** tab:

  - **Create allowing rules based on running applications**
  - **Create allowing rules for applications from the folders**

  You can specify the following actions to perform while creating Applications Launch Control allowing rules on the **Settings** tab:

  - **Use digital certificate**
  - **Use digital certificate subject and thumbprint**
  - **If the certificate is missing, use**
  - **Use SHA256 hash**
  - **Generate rules for users and / or group of users**

  You can configure settings for configuration files with allowing rule lists that Kaspersky Industrial CyberSecurity for Nodes creates upon task completion.

  You can configure settings to start the task on a schedule.

- Rule Generator for Device Control
  - Select the operation mode: consider system data about all external devices that have ever been connected or consider currently connected external devices only.
  - Configure settings for configuration files with allowing rule lists that Kaspersky Industrial CyberSecurity for Nodes creates upon task completion.
  - You can configure settings to start the task on a schedule.
- Application Activation
  - To activate the application or to renew the license, you can add a key file or activation code.
  - You can configure settings to start the task on a schedule.
- Update of databases and application modules
  - You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source in the **Update source** settings block. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.

    You can specify the usage of Kaspersky update servers, if manually customized servers are not available.
  - You can configure the settings for a feature that reduces the load on the disk subsystem:
    - **Lower the load on the disk I/O**
    - **RAM used for optimization, MB**
  - You can specify the actions that Kaspersky Industrial CyberSecurity for Nodes will perform if critical application module updates are needed, as well as after installation of critical updates is complete. In addition, you can specify whether Kaspersky Industrial CyberSecurity for Nodes will receive information about available scheduled updates.
  - You can specify the set of updates to copy and a path to the folder that will be used by Kaspersky Industrial CyberSecurity for Nodes to store copied updates.
  - You can configure settings to start the task on a schedule.
- On-Demand Scan
  - You can specify a scan scope for the On-Demand Scan task and configure security level settings.
  - In the **Heuristic analyzer** settings block, you can enable or disable use of the heuristic analyzer for the On-Demand Scan task and set the analysis level using a slider.

- In the **Integration with other components** block, you can configure the following settings:
  - Start the scan task in background mode.
  - Consider task as critical areas scan.
  - Disable simultaneous launch of several scan tasks.
- You can configure settings to start the task on a schedule.

- Application Integrity Control
  - You can configure settings to start the task on a schedule.
- Baseline System Integrity Monitor
  - You can configure the monitoring mode and the rules that specify actions to take on files, the registry, and devices.
  - You can configure settings to start the task on a schedule.

Application activation task

To configure the Application Activation task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

   In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
5. In the **Activation settings** section, specify the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add a key to renew the license.
6. In the **Schedule** section, configure task schedule settings.
7. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information on configuring settings in these sections, see Kaspersky Security Center Help.
8. Click the **OK** button in the **Properties: <Task name>** window.

The newly configured group task settings are saved.

Update task

To configure the Update task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
5. In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
6. In the **Settings** section do the following:
   a. Select an update source using the **Settings** button in the **Application databases and modules update settings** section:
      - Kaspersky Security Center Administration Server.
      - Kaspersky update servers.
      - Custom HTTP or FTP servers, or network folders.

      To use an SMB-shared folder as an update source, you need to specify a user account to start a task.

      You can specify the usage of Kaspersky update servers, if manually customized servers are not available.
   b. Configure the settings for a feature that reduces the load on the disk subsystem:
      - **Lower the load on the disk I/O**. This check box enables or disables the process whereby the disk subsystem is optimized by storing update files on a virtual drive in RAM. By default, the check box is cleared.
      - **RAM used for optimization, MB**
   c. Specify actions that Kaspersky Industrial CyberSecurity for Nodes should perform when critical updates of application modules are available or when there is information about planned updates.
   d. Specify update copying settings.
7. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Update rollback).

8. In the **Account** section, specify the account whose rights will be used to run the task.

> For detailed information on configuring settings in these sections, see Kaspersky Security Center Help.

9. In the **Properties: <Task name>** window, click **OK**.

For the *Update rollback* task, you can configure only the standard task settings controlled by Kaspersky Security Center in the **Notifications** and **Exclusions from task scope** sections. For detailed information on configuring settings in these sections, see Kaspersky Security Center Help.

Application Integrity Control

To configure the Application Integrity Control group task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
5. In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.
6. In the **Devices** section, select the devices for which you want to configure the *Application Integrity Control* task.
7. In the **Schedule** section, configure task schedule settings.
8. In the **Account** section, specify the account whose rights will be used to run the task.
9. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

> For detailed information on configuring settings in these sections, see Kaspersky Security Center Help.

10. Click the **OK** button in the **Properties: <Task name>** window.

Scheduling tasks

To schedule tasks using the Administration Plug-in:

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. Double-click to open the properties window for the task for which you want to configure the schedule.
6. Select the **Schedule** section.
7. Configure the schedule settings (see the table below) as needed.

   Fields with schedule settings for the On-Demand Scan and Update tasks are unavailable if scheduling of these tasks is blocked by a Kaspersky Security Center policy.

8. Click the **Apply** button to save the task start settings.

If you want to configure application settings for a single task using Kaspersky Security Center, see section "Configuring local tasks in the Application settings window of the Kaspersky Security Center".

Task schedule settings

Parameter	Description
Scheduled start	Select the task run mode: • **Every N hours**. The task will run periodically every few hours. Specify the start time of the task and the period in hours. • **Every N days**. The task will run periodically every few days. Specify the start time of the task and the period in days. • **Every N minutes**. The task will run periodically every few minutes. Specify the start time of the task and the period in minutes. • **Weekly**. The task will run on a certain day of the week. Specify the day of the week and the start time. • **Monthly**. The task will run on a certain day of the month. Specify the date and time of the start. • **Once**. The task will run once at the specified date and time. • **Manually**. Run mode in which you can start scan manually at a time when it is convenient for you. • **When new updates are downloaded to the repository**. The task will run every time updates are downloaded to the repository. • **On completing another task**. The task will run upon completion of another task. Select the task and its completion status. Kaspersky Industrial CyberSecurity for Nodes does not support the **On completing another task** mode for scheduling local tasks. • **On virus outbreak**. The task will run if a virus attack is detected. • **At application start**. The task will run every time Kaspersky Industrial CyberSecurity for Nodes starts.

Parameter	Description
Run missed tasks	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes starts the skipped task as soon as it becomes possible. The task may be skipped, for example, if the computer was off at the scheduled task start time. When the application gets an opportunity to execute missed tasks, it runs the tasks randomly within a certain time interval to distribute the load on the computer. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes does not run skipped tasks. Instead, it carries out the next task in accordance with the current schedule.
Use automatically randomized delay for task starts	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Use randomized delay for task starts within an interval of (min)	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Turn on devices by using the Wake-on-LAN function before starting the task	If the check box is selected, the operating system of the computer is given a specified lead time to complete startup before the task is run. The default lead time is 5 minutes. Select the check box if you want to run the task on all computers including powered off computers.
Shut down the devices after completing the task	If this check box is selected, the computer will shut down after the task is completed. For example, you can enable this functionality to scan the computer on Fridays after working hours. When the task finishes, the application turns off the computer for the weekend.
Stop the task if it runs longer than	Limiting the task execution time. After the specified amount of time, Kaspersky Industrial CyberSecurity for Nodes stops the task. The task is not marked as completed. Next time Kaspersky Industrial CyberSecurity for Nodes runs the task, it will be run from the beginning and on schedule.
Pause task	You can specify a time interval during which the execution of a previously scheduled task will be paused. Once the specified time period is over, the task will resume. This may be necessary, for example, to minimize the impact of Kaspersky Industrial CyberSecurity for Nodes on the performance of your computer during periods of peak usage. This functionality is available only for On-Demand Scan tasks.
Disable schedule from	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes will stop running the scheduled task starting on the specified date. The task will be set to **Manually** mode. This functionality is available only for On-Demand Scan tasks.

Reports in Kaspersky Security Center

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are based on information stored on Administration Server.

Starting from Kaspersky Security Center 11, the following types of reports are available for Kaspersky Industrial CyberSecurity for Nodes:

- Report on the status of application components
- Report on prohibited applications
- Report on prohibited applications in test mode

For detailed information on working with Kaspersky Security Center reports, please refer to the Kaspersky Security Center Help.

Report on the status of Kaspersky Industrial CyberSecurity for Nodes components

You can monitor the protection status of all network devices and get a structured overview of the set of components on each device.

The report displays one of the following states for each component: *Running*, *Paused*, *Stopped*, *Not covered by license*.

Not Installed status refers to the component, not the application itself. If the application is not installed, Kaspersky Security Center assigns the N/A (Not available) status.

You can create component selections and use filtering to display network devices with a specified set of components and state.

See Kaspersky Security Center Help for detailed information about creating and using selections.

To review the component statuses in the application settings:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Select the **Devices** tab and open the **Application settings** window.
3. Select the **Components** section.
4. Review the status table.

To review a Kaspersky Security Center standard report:

1. Select the **Administration Server <Administration Server name>** node in the Administration Console tree.
2. Select the **Reports** tab.
3. Double-click the **Report on the status of application components** list item.

   A report is generated.

4. Review the following report details:

   - A graphical diagram.
   - A summary table of components and aggregated numbers of network devices where each of the components is installed, and groups they belong to.
   - A detailed table specifying the component status, version, device and group.

Reports on prohibited applications in active and test modes

Based on the results of the Applications Launch Control task, two types of reports can be generated: a report on prohibited applications (if the task is started in Active mode) and a report on prohibited applications in test mode (if the task is started in the Inform mode). These reports display information about blocked applications on the protected devices of the network. Each report is generated for all administration groups and accumulates data from all the Kaspersky applications installed on the protected devices.

To review a report on prohibited applications in the Inform mode:

1. Start the Applications Launch Control task in the Inform mode.
2. Select the **Administration Server <Administration Server name>** node in the Administration Console tree.
3. Select the **Reports** tab.
4. Double-click the **Report on prohibited applications in test mode** item.

   A report is generated.
5. Review the following report details:

   - A graphical diagram that displays the top 10 applications with the largest number of blocked starts.
   - A summary table of application blocks, specifying the executable file name, reason, time of blocking, and number of devices where the blocking occurred.
   - A detailed table specifying data about the device, file path and criteria for blocking.

To review a report on prohibited applications in Active mode:

1. Run the Applications Launch Control task in Active mode.
2. Select the **Administration Server <Administration Server name>** node in the Administration Console tree.
3. Select the **Reports** tab.
4. Double-click the **Report on prohibited applications** item.

   A report is generated.

This report consists of the same data about blocks as the report on prohibited applications in test mode.

Real-Time Protection status

Kaspersky Industrial CyberSecurity for Nodes sends the setting **Real-time protection status** to the Kaspersky Security Center Administration Server; the value of this setting depends on the current state of application protection components on the protected device (see the table below).

Kaspersky Industrial CyberSecurity for Nodes determines the real-time protection status based on the status of the following application components:

- Real-Time File Protection
- Device Control
- Firewall
- Network Threat Protection
- AMSI Scanner
- Anti-Cryptor
- BadUSB Attack Prevention
- Remediation Engine
- Exploit Prevention.

You can check the real-time protection status of the application in a Kaspersky Security Center console.

How to find out the Real-Time Protection status in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Managed devices**.

   The current Real-Time Protection status is displayed in the list of devices, in the **Real-time protection status** column. If the **Real-time protection status** column is missing, manage column settings by clicking the **Add/Remove Columns** link.

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Managed devices**.

   The current Real-Time Protection status is displayed in the list of devices, in the **Real-time protection status** column. If the **Real-time protection status** column is missing, manage column settings by clicking the **Add/Remove Columns** link.

How to find out the Real-Time Computer Protection in the Web Console

In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

The current Real-Time Protection status is displayed in the list of devices, in the **Real-time protection status** column. If the **Real-time protection status** is column missing, manage column settings (⚙).

Possible values of the Real-time protection status setting

Value	Description
Unknown	The Administration Server does not have information about the real-time protection status for this device.
Not installed	No components are installed.
Not supported by license	The application is not activated or the license does not allow the installed components to work.
Failed	One or more components have malfunctioned.
Stopped	One or more components are disabled.
Paused	One or more components are paused.
Starting	One or more components are being turned on.
Running	Application components are up and running.

If the value of the **Real-time protection status** setting in Kaspersky Security Center is different from *Running*, check that the installed components of Kaspersky Industrial CyberSecurity for Nodes from the list are enabled and the application is activated.

Working with the Kaspersky Industrial CyberSecurity for Nodes Console

This section provides information about the Kaspersky Industrial CyberSecurity for Nodes Console and describes how to manage the application using the Application Console installed on the protected device or another device.

Starting the Application Console

To start the Application Console:

1. Open the Compact Diagnostic Interface in one of the following ways:

   - Run the avpui.exe file in the application installation folder on the protected device. By default, the file is located in C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.
   - Click the application icon in the taskbar notification area.

2. In the Compact Diagnostic Interface window that opens, click the **Kaspersky Industrial CyberSecurity for Nodes Console** link.

   If you have already configured a connection to the protected device, the Application Console opens.

   If you are starting the Application Console for the first time, you are taken to the **Select protected device** window, in which you must configure the connection of the Application Console to the protected computer.

   The application console version 4.5 is not compatible with Kaspersky Industrial CyberSecurity for Nodes version 5.0 and later. When attempting to connect, you will be prompted to install the compatibility pack for the Application Console. The compatibility pack will be downloaded from the device to which you are connecting.

Kaspersky Industrial CyberSecurity for Nodes Console interface

This section describes the primary elements of the application interface.

Kaspersky Industrial CyberSecurity for Nodes Console window

After a connection has been established to Kaspersky Industrial CyberSecurity for Nodes installed on a different protected device, the name of the node is supplemented with the name of the protected device on which the application is installed and the name of the user account under which the connection has been established: **Kaspersky Industrial CyberSecurity for Nodes <Name of protected device> as <account name>**. Upon connection to Kaspersky Industrial CyberSecurity for Nodes installed on the same protected device with the Kaspersky Industrial CyberSecurity for Nodes Console, the node name is Kaspersky Industrial CyberSecurity for Nodes.

Console tree

The Application Console tree displays the Kaspersky Industrial CyberSecurity for Nodes node and the child nodes of functional components of the application.

The **Kaspersky Industrial CyberSecurity for Nodes** node includes the following child nodes:

- **Real-Time Computer Protection** allows configuring the following tasks:
  - **Real-Time File Protection**
  - **Kaspersky Security Network**
  - **Exploit Prevention**
  - **Network Threat Protection**
  - **Anti-Cryptor**
  - **Remediation Engine**
  - **AMSI Scanner**
- **Telemetry settings**: settings for telemetry sent by the application to compatible Detection and Response solutions and SIEM systems.
- **Computer Control**: control of applications running on the protected device and connected devices.
  - **Applications Launch Control**
  - **Device Control**
  - **Firewall**
- **Automatic Rule Generation**: configuring automatic generation of group and system rules for the Applications Launch Control component and the Device Control component.
  - **Rule Generator for Applications Launch Control**
  - **Rule Generator for Device Control**

- Rule generation group tasks **<Task names>** (if any)

  Group tasks are created using Kaspersky Security Center. You cannot manage group tasks through Kaspersky Industrial CyberSecurity for Nodes Console.

- **System Inspection**: configuring the settings of system integrity monitoring and Windows event log analysis.
  - **Log Inspection**
  - **System Integrity Monitoring**
- **Industrial Network Protection**: receives information about protected PLCs and monitors their integrity.
  - **PLC Project Integrity Check**
  - **PLC Project Investigation**
- **On-Demand Scan**: manages On-Demand Scan tasks. There is a separate node for each task:
  - **Scan at Operating System Startup**
  - **Critical Areas Scan**
  - **Application Integrity Control**
  - **Removable Drives Scan**
  - **Full Scan**
  - Custom tasks **<Task names>** (if any)

  The node displays system tasks created when the application is installed, custom tasks, and group on-demand scan tasks created and sent to a protected device using Kaspersky Security Center.

- **Update**: manages updates for Kaspersky Industrial CyberSecurity for Nodes databases and application modules, and provides the possibility to roll back the last update:
  - **Update of databases and application modules**
  - **Last update rollback**
  - **Application update**

  The node displays all custom and group update tasks created and sent to a protected device using Kaspersky Security Center.

- **Storages**: manages Backup settings and the list of blocked network sessions.
  - **Backup**
  - **Blocked network sessions**

- **Logs and notifications**: manages local task logs and Kaspersky Industrial CyberSecurity for Nodes System audit log.
  - **System Audit**
  - **Industrial Network Protection**
  - **Applications Launch Control**
  - **Device Control**
  - **Application Integrity Control**
  - **Log Inspection**
  - **System Integrity Monitoring**
  - **Network Threat Protection**
  - **On-Demand Scan**
  - **Firewall**
  - **Exploit Prevention**
  - **Anti-Cryptor**
  - **AMSI Scanner**
  - **Update**
  - **Real-Time File Protection**
  - **Backup**
  - **Endpoint Detection and Response (Industrial CyberSecurity)**
- **Licensing**: add or delete Kaspersky Industrial CyberSecurity for Nodes keys, view license details.

Details pane

The details pane displays information about the selected node. If the **Kaspersky Industrial CyberSecurity for Nodes** node is selected, the details pane displays information about the current device protection status and information about Kaspersky Industrial CyberSecurity for Nodes, the protection status of its functional components, and the key status.

Context menu of the Kaspersky Industrial CyberSecurity for Nodes node

You can use the items of the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node to perform the following operations:

- **Pause protection**.
- **Trusted zone**. View and configure Trusted Zone settings.
- **Telemetry settings for KATA Integration / Integration with KICS for Networks**.
- **Removable Drives Scan**. Configure scanning of removable drives connected to the protected device via the USB port.
- **User access permissions for application management**. View and configure permissions to access Kaspersky Industrial CyberSecurity for Nodes functions.
- **User access permissions for KICS for Nodes Service management**. View and configure user rights to manage the Kaspersky Industrial CyberSecurity for Nodes Service.
- **Storages**.
- **Export settings**. Save the application settings in a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Import settings**. Import application settings from a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Refresh**. Refresh the contents of the Kaspersky Industrial CyberSecurity for Nodes Console window. You can also perform this operation in context menus of application tasks.
- **Application properties**. View and configure settings of Kaspersky Industrial CyberSecurity for Nodes or a selected task. You can also perform this operation in context menus of application tasks.

  To do so, you can also use the **Application properties** link in the details pane of the Kaspersky Industrial CyberSecurity for Nodes node.

- **Help**. View information in Kaspersky Industrial CyberSecurity for Nodes Help. You can also perform this operation in context menus of application tasks.

Toolbar and context menu of Kaspersky Industrial CyberSecurity for Nodes tasks

You can manage the application tasks using the items of context menus of each task in the Kaspersky Industrial CyberSecurity for Nodes Console tree.

You can use the items of the context menu to perform the following operations:

- **Resume/Pause**. Resume or pause task execution. To carry out these operations, you can also use the buttons on the toolbar. This operation is available for the Real-Time Protection tasks and the On-Demand Scan tasks.
- **Create task**. Create new custom task.
- **Delete task**. Delete custom task.
- **Export settings** / **Import settings**. Export or import task settings.
- **Properties**. Open the task settings window.
- **Help**. Open the corresponding online help topic.

System Tray Icon in the notification area

Immediately after installation of Kaspersky Industrial CyberSecurity for Nodes, the application icon appears in the Microsoft Windows taskbar notification area.

> If the application icon in the taskbar notification area is hidden, the administrator has disabled the display of the application interface in the policy.

The icon serves the following purposes:

- It indicates application activity.
- It acts as a shortcut to the context menu and main window of the application.

The following application icon statuses are provided for displaying application operating information:

- The icon signifies that critically important protection components of the application are enabled. Kaspersky Industrial CyberSecurity for Nodes will display a warning if the user is required to perform an action, for example, restart the computer after updating the application.
- The icon signifies that critically important protection components of the application are disabled or have malfunctioned. Protection components may malfunction, for example, if the license has expired or as a result of an application error. Kaspersky Industrial CyberSecurity for Nodes will display a warning with a description of the problem in computer protection.

You can open the context menu of the System Tray Icon by right-clicking it.

The context menu offers several commands to display application windows (see table below).

Context menu commands in System Tray Icon

Command	Description
Open Application Console	Opens Kaspersky Industrial CyberSecurity for Nodes Console (if installed).
Open Compact Diagnostic Interface	Opens the Compact Diagnostic Interface.

Command	Description
About	Opens the **About** window containing information about Kaspersky Industrial CyberSecurity for Nodes. For registered Kaspersky Industrial CyberSecurity for Nodes users, the **About** window contains information about urgent updates that have been installed.
Hide	Hides the System Tray Icon in the toolbar notification area.

You can display the hidden System Tray Icon again at any time.

To display the System Tray Icon again,

in the Microsoft Windows **Start** menu, select **All Programs** > **Kaspersky Industrial CyberSecurity for Nodes**. The icon will appear in the notification area of the Microsoft Windows taskbar.

The names of settings may vary depending on the installed operating system.

Configuring general settings via the Application Console

General settings and malfunction diagnostics settings of Kaspersky Industrial CyberSecurity for Nodes establish the general operating conditions for the application. These settings allow you to control the number of working processes used by Kaspersky Industrial CyberSecurity for Nodes, enable recovery of Kaspersky Industrial CyberSecurity for Nodes tasks after an abnormal termination, maintain the log, enable creation of dump files of Kaspersky Industrial CyberSecurity for Nodes processes after abnormal termination, and configure other general settings.

Application settings cannot be configured in the Kaspersky Industrial CyberSecurity for Nodes Console if the active Kaspersky Security Center policy blocks changes to these settings.

To configure the general settings of Kaspersky Industrial CyberSecurity for Nodes:

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and do one of the following:

   - Click the **Application properties** link in the results pane of the node.
   - Select **Application properties** in the node's context menu.

   The **Application properties** window opens.

2. On the **Interface** tab, specify which warnings you want to see on the Kaspersky Industrial CyberSecurity for Nodes system tray icon.

3. On the **Security settings** tab, configure the following settings:

   - In the **General** section, configure the **Start the application on computer startup (recommended)** option.
   - Under **Self-Defense**, configure the protection of application modules and operating system services.

- In the **Actions when switching to UPS backup power** section, specify limitations on protected device load created by Kaspersky Industrial CyberSecurity for Nodes after switching to UPS power:
  - **Do not start scheduled scan tasks**.
  - **Stop running scan tasks**.
- In the **Compatibility settings** section, configure the **Compatibility with remote administration software** setting.
- In the **Scan settings** section, configure the CPU usage limit for scan tasks and allow conceding resources to other applications.

4. On the **Network settings** tab, configure the following settings:
   - In the **Proxy server** section, specify the proxy server settings: authentication type and details required for authentication on the proxy server.
   - Under **Monitored ports**, specify the network port monitoring option:
     - **Monitor all network ports**. In this network port monitoring mode the protection components monitor data streams that are transmitted via any open network ports of the computer.
     - **Monitor selected network ports only**. In this network port monitoring mode, the protection components monitor the selected ports of the computer and the network activity of the selected applications. The list of network ports that are normally used for transmission of email and network traffic is configured according to the recommendations of Kaspersky experts. If necessary you can edit the list of network ports.
   - Under **Port for remote connection**, if necessary, change the ports that the Application Console uses to connect to the computer with the application installed.

     The default port number for connection with Windows credentials is 13032, and the default port number for connection with credentials of manually created users is 13031. Range of possible port numbers: 1–65535.

     The previously saved port numbers are used until the application is restarted.
5. On the **Malfunction diagnosis** tab, click **Settings** and configure the tracing and memory dumping of the application.
6. Click **OK**.

Kaspersky Industrial CyberSecurity for Nodes settings are saved.

Managing Kaspersky Industrial CyberSecurity for Nodes tasks

This section contains information about how to create, configure, start, and stop Kaspersky Industrial CyberSecurity for Nodes tasks.

Kaspersky Industrial CyberSecurity for Nodes task categories

Real-Time Computer Protection, Computer Control, Automatic Rule Generation, System Inspection, On-Demand Scan, Industrial Network Protection, Storage management and Update functions in Kaspersky Industrial CyberSecurity for Nodes are implemented as tasks.

You can manage these tasks using the task context menu in the Kaspersky Industrial CyberSecurity for Nodes Console tree, and the results pane. You can view task status information in the results pane. Task management operations are recorded in the system audit log.

There are two types of Kaspersky Industrial CyberSecurity for Nodes tasks: *local* and *group*.

Local tasks

Local tasks can only be executed on the protected device they were created for. Depending on the start method, the following types of local tasks exist:

- **Local system tasks**. These tasks are created automatically during installation of Kaspersky Industrial CyberSecurity for Nodes. You can change the settings of all local system tasks except the *Update rollback* task. Local system tasks cannot be renamed or deleted. You can run local system and custom On-Demand Scan tasks simultaneously.

- **Local custom tasks**. In the Application Console, you can create On-Demand Scan tasks, Update tasks, and Baseline System Integrity Monitor tasks. In Kaspersky Security Center, you can create On-Demand Scan tasks, Update tasks, etc. You can rename, configure, or delete custom tasks. You can run several custom tasks simultaneously.

Group tasks

You can manage group tasks and tasks for sets of protected devices from the Kaspersky Security Center. All group tasks are custom tasks. Group tasks are also displayed in the Application Console. In the Application Console, you can only view the status of group tasks. You cannot use the Application Console to manage or configure group tasks.

Starting, pausing, resuming, and stopping tasks manually

You can start, pause, resume or stop tasks manually. These options are not available for all Kaspersky Industrial CyberSecurity for Nodes tasks.

To start, pause, resume or stop a task:

1. In the Application Console, open the context menu of the task.
2. Select one of the following commands: **Start**, or **Pause**.

The operation is performed and recorded in the system audit log.

Scheduling tasks

In the Kaspersky Industrial CyberSecurity for Nodes Console, you can configure a schedule for running local system and user tasks. However, you cannot configure a schedule for running group tasks.

To schedule a task:

1. In the Console tree, select the task for which you want to configure the schedule.
2. In the results pane, click the **Properties** link.
3. In the window that opens, in the **Run mode** section, perform one of the following actions:
   - Select the **Manually** check box to run the task manually at a time that is convenient for you.
   - Select the **By schedule** check box if you want to enable scheduled task start.
4. If you select the **By schedule** option, configure the task schedule settings (see the table below).
5. If necessary, select the **Run task as** check box and specify the credentials of the user account that will be running the task.
6. Click **OK**.

The task schedule settings are saved.

Task schedule settings

Parameter	Description
Run mode	Select the task run mode: • **Minutes**. The task will run periodically every few minutes. Specify the start time of the task and the period in minutes. • **Hours**. The task will run periodically every few hours. Specify the start time of the task and the period in hours. • **Days**. The task will run periodically every few days. Specify the start time of the task and the period in days. • **Weeks**. The task will run on the specified days of the week at intervals of a specified number of weeks. Specify the schedule, use the check boxes to select the days of the week on which the task will run, and specify the start time for the task. • **Every month**. The task will run on a certain day of the month. Specify the date and time of the start. • **At a specified time**. The task will run once at the specified date and time. • **After every update**. The task will run every time updates are downloaded to the repository. • **After application startup**. The task will run every time Kaspersky Industrial CyberSecurity for Nodes starts.
Run missed tasks	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes starts the skipped task as soon as it becomes possible. The task may be skipped, for example, if the computer was off at the scheduled task start time. When the application gets an opportunity to execute missed tasks, it runs the tasks randomly within a certain time interval to distribute the load on the computer. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes does not run skipped tasks. Instead, it carries out the next task in accordance with the current schedule.

Parameter	Description
Use automatically randomized delay for task starts	If the check box is selected, the task is not run strictly on schedule, but randomly within a certain interval, that is, the start times of the task are spread out. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. The range of randomized start times is automatically calculated when the task is created, depending on the number of computers that have the task assigned. Subsequently, the task is always run at its calculated start time. However, whenever task settings are modified or the task is run manually, the calculated start time changes. If the check box is cleared, the task is run exactly at scheduled time.
Use randomized delay for task starts within an interval of (min)	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Pause task	You can specify a time interval during which the execution of a previously scheduled task will be paused. Once the specified time period is over, the task will resume. This may be necessary, for example, to minimize the impact of Kaspersky Industrial CyberSecurity for Nodes on the performance of your computer during periods of peak usage. This functionality is available only for On-Demand Scan tasks.
Disable schedule from	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes will stop running the scheduled task starting on the specified date. The task will be set to **Manually** mode. This functionality is available only for On-Demand Scan tasks.

Using user accounts to start tasks

You can start tasks under the system account or specify a different account.

About using accounts to start tasks

You can specify the account to run the following Kaspersky Industrial CyberSecurity for Nodes tasks:

- *Rule Generator for Applications Launch Control*
- *Rule Generator for Device Control*
- *Log Inspection*
- *Application Integrity Control*
- *Update*.

By default, these tasks are run using system account permissions.

A different account with proper access permissions is recommended in the following cases:

- For the *Update* task:
  - If you specified a shared folder on a different device on the network as the update source.
  - If you use a proxy server with NTLM or Kerberos authentication for access to the update source.
- For the *Rule Generator for Applications Launch Control* task: if the generated rules are exported to a configuration file that the system account cannot access (for example, in a shared folder on the protected device).

You can start listed tasks with system account privileges. Kaspersky Industrial CyberSecurity for Nodes performs these tasks and accesses shared folders on another device in the network if this device is registered in the same domain as the protected device. In this case, the system account must have access permissions for these folders. Kaspersky Industrial CyberSecurity for Nodes accesses the device using permissions for the account **<domain name \ device_name>**.

Specifying a user account to start a task

The option to specify an account in the Application Console is not available for all tasks.

To specify an account to start a task:

1. In the Application Console tree, select the task you want to start with the rights of a specific account.
2. In the results pane, click the **Properties** link.
   The **Properties: <Task name>** window opens.
3. Go to the **Run mode** tab and do the following:
   a. Select the **Run task as** check box.
   b. Enter the user name and password for the account you want to use.

      The selected user must be registered on the protected device or in the same domain as this computer.
4. Click **OK**.

Importing and exporting settings

This section explains how to export Kaspersky Industrial CyberSecurity for Nodes settings. You will also learn how to export settings of certain application components to an XML configuration file, and how to import these settings from a configuration file back into the application.

About importing and exporting settings

You can export Kaspersky Industrial CyberSecurity for Nodes settings to an XML configuration file and import settings into Kaspersky Industrial CyberSecurity for Nodes from the configuration file. You can save all application settings or only settings for individual components to a configuration file.

When you export all settings of Kaspersky Industrial CyberSecurity for Nodes to a file, the general application settings and settings of the following Kaspersky Industrial CyberSecurity for Nodes components and functions are saved:

- Real-Time File Protection
- Exploit Prevention
- Network Threat Protection
- Anti-Cryptor
- Remediation Engine
- AMSI Scanner
- Applications Launch Control
- Device Control
- Firewall
- Rule Generator for Applications Launch Control
- Rule Generator for Device Control
- Log Inspection
- System Integrity Monitoring
- PLC Project Integrity Check
- PLC Project Investigation
- Scan at Operating System Startup
- Critical Areas Scan
- Application Integrity Control
- Removable Drives Scan
- Full Scan
- Updating databases and application software modules

- Last update rollback
- Update

Also, you can save the general settings of Kaspersky Industrial CyberSecurity for Nodes in the file, as well as the rights of user accounts.

If a Kaspersky Security Center policy is active at the time of export, the application exports the specified values used by that policy.

You cannot export group task settings.

Kaspersky Industrial CyberSecurity for Nodes exports all passwords used by the application, for example, user account settings for running tasks or connecting to a proxy server. Exported passwords are saved in encrypted form in the configuration file. You can import passwords only using Kaspersky Industrial CyberSecurity for Nodes installed on this protected device if it has not been reinstalled or updated.

You cannot import previously saved passwords using Kaspersky Industrial CyberSecurity for Nodes installed on a different protected device. After settings have been imported on the protected device, all passwords must be entered manually.

If the **Request password to confirm critical actions** functionality was enabled when exporting settings, the password set on the device is exported and then automatically applied on the other device when importing settings.

Settings can be imported from a configuration file containing settings for individual Kaspersky Industrial CyberSecurity for Nodes components (e.g. from a file created in Kaspersky Industrial CyberSecurity for Nodes installed with an incomplete set of components). After the settings are imported, only those Kaspersky Industrial CyberSecurity for Nodes settings that were contained in the configuration file are changed. All other settings remain the same.

Settings of an active Kaspersky Security Center policy that have been blocked do not change when importing the settings.

Exporting settings

To export settings to a configuration file:

1. To export all Kaspersky Industrial CyberSecurity for Nodes settings, in the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node, select the **Export settings** command.

   To export the settings of an individual component, click **Export settings** in the results pane.

   Kaspersky Security Network settings cannot be exported. Kaspersky Security Network must be configured manually.

2. In the window that opens, specify the name of the XML file to which you want to export the list of settings, and select the folder in which you want to save this file.

   You can use system environment variables when specifying the path, but not user environment variables.

If a Kaspersky Security Center policy is active at the time of export, the application exports the settings used by that policy.

3. Save the file.

4. Click the **OK** button in the **Export of settings is successfully completed** window.

   Kaspersky Industrial CyberSecurity for Nodes exports the list of settings to the XML file.

To export the list of trusted applications:

1. In the Application Console tree, open the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.

2. Select **Configure Trusted zone settings**.

3. The **Configure Trusted zone settings** window opens.

4. Go to the **Trusted applications** section and click **Settings**.

   This opens a window containing a list of trusted applications.

5. Select the trusted applications that you want to export.

   If you do not select any trusted application, Kaspersky Industrial CyberSecurity for Nodes exports all trusted applications.

6. Click the arrow and in the drop-down list, select **Export**.

7. This opens a window; in that window, enter the name of the XML file to which you want to export the list of trusted applications, and select the folder in which you want to save this file.

8. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the list of trusted applications to the XML file.

You can also export the Kaspersky Industrial CyberSecurity for Nodes settings using the command line.

Importing settings

To import settings from a saved configuration file:

1. To import all Kaspersky Industrial CyberSecurity for Nodes settings, in the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node, select the **Import settings** command.

   To import the settings of an individual component, click **Import settings** in the results pane.

After importing the general Kaspersky Industrial CyberSecurity for Nodes settings or its functional component settings to the protected device, you cannot revert to the previous settings.

Kaspersky Security Network settings cannot be imported. Kaspersky Security Network must be configured manually.

2. In the displayed window, select the XML configuration file from which you want to import settings and click **Open**.

3. Click the **OK** button in the **Import of settings is successfully completed** window.

4. In the Application Console toolbar, click the **Update** button.

   The Application Console window displays the imported settings.

Kaspersky Industrial CyberSecurity for Nodes does not import passwords (account credentials for starting tasks or connecting to the proxy server) from a file created on another protected device or on the same protected device after Kaspersky Industrial CyberSecurity for Nodes has been re-installed or updated on it. After import is complete, passwords must be entered manually.

To import the list of trusted applications:

1. In the Application Console tree, open the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.

2. Select **Configure Trusted zone settings**.

3. The **Configure Trusted zone settings** window opens.

4. Go to the **Trusted applications** section and click **Settings**.

5. Click the arrow and in the drop-down list, select **Import**.

6. This opens a window; in that window, select the XML file from which you want to import the list of trusted applications.

7. Open the file.

   If the computer already has a list of trusted applications, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

8. The list is displayed on the **Trusted applications** tab. Click **OK**.

Viewing protection status and Kaspersky Industrial CyberSecurity for Nodes information

To view information about the device protection status Kaspersky Industrial CyberSecurity for Nodes,

select the **Kaspersky Industrial CyberSecurity for Nodes** node in the Kaspersky Industrial CyberSecurity for Nodes Console tree.

By default, information in the details pane of Kaspersky Industrial CyberSecurity for Nodes Console is refreshed automatically:

- Every 10 seconds in case of a local connection.
- Every 15 seconds in case of a remote connection.

You can refresh information manually.

*To refresh information in the **Kaspersky Industrial CyberSecurity for Nodes** node manually,*

select the **Refresh** command in the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.

The following application information is displayed in the details pane of Kaspersky Industrial CyberSecurity for Nodes Console:

- Kaspersky Security Network Usage status.
- Device protection status.
- Information about database and application module updates.
- Actual diagnostics data.
- Data about protected device control tasks.
- License information.
- Status of the Industrial network protection.
- Status of integration with Kaspersky Security Center: details of the server with Kaspersky Security Center installed, to which the application is connected; information about application tasks controlled by the active policy.

Color coding is used to display the protection status:

- *Green*. The task is being run in accordance with the configured settings. Protection is active.
- *Yellow*. The task was not started, has been paused, or has been stopped. Security threats may occur. You are advised to configure and start the task.
- *Red*. The task completed with an error or a security threat was detected while the task was running. You are advised to start the task or take measures to eliminate the detected security threat.

Some details in this block (for example, task names or the number of threats detected) are links that, when clicked, take you to the node of the relevant task or open the task log.

The **KSN Usage** section displays current task status, for example, *Running*, *Stopped* or *Never performed*. The indicator can take the following values:

- Green color of the panel – signifies that the **KSN Usage** task is running and file requests for statuses are being send to KSN.
- Yellow color of the panel – one of the Statements is accepted, but the task is not running, or the task is running, but file requests are not sent to KSN.
- Red color of the panel – task failed.

Computer protection

The **Computer protection** section (see the table below) displays information about the current protection status of the device.

Information about device protection status

Protection section	Information
Device protection status indicator	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green color of the panel – displayed by default and signifies that the Real-Time File Protection component is installed and the task is running. • Yellow color of the panel – signifies that the Real-Time File Protection component is not installed, and the *Critical Areas Scan* task has not been performed for a long time. • Red color of the panel – Real-Time File Protection tasks are not running.
Real-Time File Protection	**Status** – current status of the component, for example, *Running* or *Disabled*.
Critical Areas Scan	**Last scan date** – the date and time of the last Critical Areas Scan for viruses and other computer security threats. *Never performed* – an event that occurs when the *Critical Areas Scan* task has not been performed in the last 30 days or longer (default value). You can change the threshold for generating this event.
Network Threat Protection	**Status** – current status of the component, for example, *Running* or *Disabled*.
Exploit Prevention	**Status** – current status of the component, for example, *Running* or *Disabled*. **Operation mode** – one of the two available modes for the Exploit Prevention component: **Block** or **Inform**.
Anti-Cryptor	**Status** – current status of the component, for example, *Running* or *Disabled*. **Operation mode** – one of the three available modes for the Anti-Cryptor component: **Delete**, **Block**, or **Inform**.

Update

The **Update** section (see the table below) displays information about how current databases and application modules are.

Information about the status of Kaspersky Industrial CyberSecurity for Nodes databases and modules

Update section	Information
Status indicator of databases and application modules	The color of the panel with the name of the section reflects the status of databases and application modules. The indicator can take the following values: • Green color of the panel – displayed by default and signifies that application databases are up to date and that the last database and modules update task was completed successfully. • Yellow color of the panel – signifies that databases are out of date, or the last database and modules update task failed. • Red color of the panel – the event *Databases are extremely out of date* or *Databases are up to date* has occurred.
Database status	The option can take the following values: • **Databases are up to date** – application databases were updated no more than 7 days ago (default). • **Databases are out of date** – application databases were updated between 7 and 14 days ago (default). • **Databases are extremely out of date** – application databases were updated more than 14 days ago (default). You can change the thresholds for generating the *Databases are out of date* and *Databases are extremely out of date* events.
Database release date	The date and time of release of the latest databases update. The date and time are specified in UTC format.
Status of the latest completed Database Update task	The date and time of the latest database update. The date and time are specified according to the local time of the protected device. The value in the field is colored red if the *Failed* event occurs.

Control

The **Control** section (see table below) displays information about the Applications Launch Control, Device Control, and Firewall tasks.

Information about protected device control status

Control section	Information
Status indicator for protected device control	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green color of the panel – displayed by default and signifies that all the Applications Launch Control component and is installed and task is running in the Active mode; Exploit Prevention functionality is installed and active. • The panel is yellow under one or more of the following conditions: Exploit Prevention is not running; Applications Launch Control is running in the Inform mode; Exploit Prevention is running in Active mode and Applications Launch Control is not running or failed. • Red color of the panel – the Applications Launch Control task is not running or failed and Exploit Prevention is not running or in the **Inform** mode.
Applications Launch Control	**Status** – current status of the component, for example, *Running* or *Disabled*. **Operation mode** – one of the two available modes for the Applications Launch Control task: **Inform** or **Block**.
Device Control	**Status** – current status of the component, for example, *Running* or *Disabled*. **Operation mode** – one of the two available modes for the Device Control task: **By rules** or **Inform**.
Firewall	**Status** – current status of the component, for example, *Running* or *Disabled*.

Diagnostics

The **Diagnostics** section (see the table below) displays information about the System Integrity Monitoring and Log Inspection tasks.

Information about System Inspection status

Diagnostics section	Information
Diagnostics status indicator	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – displayed by default and signifies that one or both system inspection components are installed and tasks are running. • Yellow – both components are installed, but one of the system inspection tasks is not running; the *Not running* event occurs. • Red – one of the tasks failed.
System Integrity Monitoring	**Status** – current status of the component, for example, *Running* or *Disabled*.
Log Inspection	**Status** – current status of the component, for example, *Running* or *Disabled*.

Industrial Network Protection tab

The **PLC Project Investigation** section displays information about the list of PLCs that are included in the protection scope.

Information about receiving PLCs data

PLC Project Investigation section	Information
PLC in protection area status indicator	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – signifies that the task has been completed successfully at least once. • Yellow – signifies that the investigation was never performed. • Red – task failed.
PLC Project Investigation	**Status** – current status of the component, for example, *Running* or *Disabled*.

The **PLC Project Integrity Check** section displays information about number of protected PLCs and events of integrity violations.

Information about the PLC Project Integrity Check task

PLC Project Integrity Check section	Information
PLC Integrity status indicator	The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – signifies that the task has been completed successfully at least once. • Yellow – signifies that the integrity check was never performed. • Red – task failed.
PLC Project Integrity Check	**Status** – current status of the component, for example, *Running* or *Disabled*.

The Kaspersky Industrial CyberSecurity for Nodes licensing information is displayed in the row in the bottom-left corner of the details pane of the **Kaspersky Industrial CyberSecurity for Nodes** node.

You can configure Kaspersky Industrial CyberSecurity for Nodes properties by following the Application properties link.

You can connect to a different protected device by following the Connect to a remote computer link.

How to configure Backup settings in the Application Console

To configure general Backup settings:

1. In the Application Console tree, open the context menu on the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Storages**.

2. Configure the settings described in the table below.

Storage settings

Parameter	Description
On the **Reports** tab, specify the reports settings:	
Store reports no longer than	If the check box is selected, the maximum report storage term is limited to the defined time interval. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file.
Limit the size of report file to	If the check box is selected, the maximum report file size is limited to the defined value. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file when the maximum report file size is reached.
On the **Backup** tab, specify the Backup settings:	

Parameter	Description
Store objects no longer than	If the check box is selected, the maximum file storage term is limited to the defined time interval. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Industrial CyberSecurity for Nodes deletes the oldest files from Backup.
Limit the size of Backup to	If the check box is selected, the maximum storage size is limited to the defined value. By default, the maximum size is 400 MB. To avoid exceeding the maximum storage size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest files from storage when the maximum storage size is reached.
Threshold value for available space	The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value is 100 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the amount of free space in Backup. The **Threshold value for available space** check box is active if the **Limit the size of Backup to** check box is selected.

Working with the Web Plug-in from Web Console

This section provides information about the Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in for Web Console and describes how to manage the application installed on a protected device or on a group of protected devices.

Managing Kaspersky Industrial CyberSecurity for Nodes from Web Console

You can centrally manage several protected devices that have Kaspersky Industrial CyberSecurity for Nodes installed and are joined in an administration group using the Kaspersky Industrial CyberSecurity for Nodes Web Plug-in. Kaspersky Security Center Web Console also lets you separately configure the settings of each protected device included in the administration group.

An *administration group* is created manually on Kaspersky Security Center Web Console. The group includes several devices with Kaspersky Industrial CyberSecurity for Nodes installed for which you want to configure the same control and protection settings. For details on using administration groups, see Kaspersky Security Center Help.

Application settings for a single protected device are unavailable if the operation of Kaspersky Industrial CyberSecurity for Nodes on the protected device is controlled by an active Kaspersky Security Center policy.

Kaspersky Industrial CyberSecurity for Nodes can be managed from Kaspersky Security Center Web Console in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of devices. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the Properties: <Protected device name> window of Kaspersky Security Center Web Console. Policies can be used to configure general application settings, settings for real-time computer protection tasks, activity control tasks on devices, network storage protection tasks and settings for starting local system tasks on a schedule.

- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of devices. You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for protected devices that do not belong to any administration group.

- **Using the properties window of a single device**. In the device properties window, you can remotely configure the task settings for a single protected device included in an administration group. You can also configure both general application settings and settings for all Kaspersky Industrial CyberSecurity for Nodes tasks if the selected protected device is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center Web Console allows you to configure application settings and advanced features, and also to work with logs and notifications. You can configure these settings for a group of protected devices and for individual protected devices.

Web Plug-in limitations

Kaspersky Industrial CyberSecurity for Nodes Web Plug-in has the following limitations compared to Kaspersky Industrial CyberSecurity for Nodes Administration Plug-in:

- The Applications Launch Control component rules cannot be created using digital certificate or Kaspersky Security Center events.
- The Device Control component rules cannot be generated based on connected devices or system data.

Managing application settings

This section contains information about configuring Kaspersky Industrial CyberSecurity for Nodes general settings in the Kaspersky Security Center Web Console.

Configuring general application settings in Web Plug-in

You can configure Kaspersky Industrial CyberSecurity for Nodes general settings in Web Plug-in for a group of protected devices or one protected device.

Configuring interface and scan settings in Web Plug-in

To configure application interface settings:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application Settings** section.
5. Click **Configure** in the **Interface settings** subsection.
6. Configure the settings described in the table below.

User interaction settings and scan settings

Parameter	Description
Interaction with user	**Do not display user interface**. On a client computer, no signs of Kaspersky Industrial CyberSecurity for Nodes operation are displayed. The icon in the Windows notification area and notifications are not available. **Display user interface**. On the client computer, an icon is available in the Windows tray. In the context menu of the icon, the user can perform operations with Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes also displays notifications above the application icon. The context menu of the icon in the Windows system tray lets you open the Compact Diagnostic Interface. Clicking a link in the Compact Diagnostic Interface opens the Application Console.
Show application's status in notifications area	Select the check boxes opposite those categories of events about which you want to see notifications in the notification area of Microsoft Windows.

Configuring security and reliability settings in Web Plug-in

To configure security settings manually, take the following steps:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application Settings** section.
5. Click **Configure** in the **Security and reliability** subsection.
6. Configure the settings described in the table below.

Security and reliability settings

Parameter	Description
Start the application on computer startup (recommended)	When the check box is selected, Kaspersky Industrial CyberSecurity for Nodes is started after the operating system loads, protecting the computer during the entire session. When the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes is not started after the operating system loads, until the user starts it manually. Computer protection is disabled and user data may be exposed to threats.
Protect application processes from external threats	When this check box is selected, Kaspersky Industrial CyberSecurity for Nodes prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.
Protect operating system services	If the protection of operating system services is enabled, third-party applications cannot act upon the processes of the operating system. If the protection of operating system services is disabled, third-party applications can act upon the processes of the operating system.

Parameter	Description
Postpone scheduled tasks while running on battery power	If this option is selected, power-saving mode is enabled. Kaspersky Industrial CyberSecurity for Nodes postpones scheduled tasks. You can start a scan and update tasks manually, if necessary. When power-saving mode is enabled and a computer is running on battery power, the following tasks are not run, even if scheduled: • *Update of databases and application modules* • *Full Scan* • *Critical Areas Scan* • *Custom Scan* • *Application Integrity Control* • *IOC Scan*.
Computer status when settings are applied	Settings for displaying the statuses of client computers with Kaspersky Industrial CyberSecurity for Nodes installed in the Web Console when errors occur while applying a policy or executing a task. The following statuses are available: *OK*, *Warning* and *Critical*.
Compatibility with remote administration software	If using Kaspersky Industrial CyberSecurity for Nodes alongside Remote Administration Tools (RAT) causes problems, you can enable the compatibility mode. The problems may be related to the incompatibility of RATs with the Secure Desktop functionality of the application. The purpose of this functionality is to confirm actions that can potentially lower the security level of the computer. This functionality lets an application display a confirmation dialog that is isolated from other processes. This functionality uses elevated rights to secure the request. In this way, only the user can confirm the action and not the malware. If this option is selected, the RAT compatibility mode is enabled. The application displays a confirmation dialog without this functionality. This can reduce the security level of the computer. We do not recommend enabling the compatibility mode if Kaspersky Industrial CyberSecurity for Nodes is not causing problems with your RAT. If this option is cleared, the RAT compatibility mode is disabled. By default, the check box is cleared. Example: When using the browser in RemoteApp mode, Kaspersky Industrial CyberSecurity for Nodes may not display a confirmation window when visiting a website with an untrusted certificate because RemoteApp does not support the Secure Desktop functionality of the application. This can cause the browser to become unresponsive. For the browser to work correctly in RemoteApp mode, you must enable the compatibility mode. You can also try enabling the compatibility mode if you encounter problems with the Secure Desktop functionality when using other third-party software.
Limit CPU usage for scan tasks	Kaspersky Industrial CyberSecurity for Nodes limits its use of the protected device CPU during on-demand scan tasks to the value specified in the **Upper limit** field. However, the application may use much more CPU time because of other components. Enabling this functionality may negatively affect the performance of Kaspersky Industrial CyberSecurity for Nodes. By default, this function is disabled.
Yield resources to other applications	Consumption of computer resources by Kaspersky Industrial CyberSecurity for Nodes when scanning the computer may increase the load on the CPU and hard drive subsystems. This may slow down other applications. To optimize the performance, Kaspersky Industrial CyberSecurity for Nodes provides a mode for transferring resources to other applications. In this mode, the operating system can decrease the priority of Kaspersky Industrial CyberSecurity for Nodes scan task threads when the CPU load is high. This allows redistributing operating system resources to other applications. Thus, scan tasks will receive less CPU time. As a result, Kaspersky Industrial CyberSecurity for Nodes will take longer to scan the computer. By default, the application is configured to concede resources to other applications.

Configuring connection settings in Web Plug-in

The configured connection settings are used to connect Kaspersky Industrial CyberSecurity for Nodes to update and activation servers and during integration of applications with Kaspersky Security Network services.

To configure the connection settings take the following steps:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application Settings** section.
5. Click **Configure** in the **Connection settings** subsection.
6. Configure the settings described in the table below.

Connection settings

Parameter	Description
Limit traffic on a metered connection	If this check box is selected, the application limits its own network traffic when the Internet connection is limited. Kaspersky Industrial CyberSecurity for Nodes identifies a high-speed mobile Internet connection as a limited connection and identifies a Wi-Fi connection as an unlimited connection. Cost-Aware Networking works on computers running Windows 8 or later.
Do not use a proxy server	If this option is selected, Kaspersky Industrial CyberSecurity for Nodes does not use a proxy server.
Automatically detect proxy server settings	If this option is selected, Kaspersky Industrial CyberSecurity for Nodes uses proxy settings of the operating system.
Use specified proxy server settings	If this option is selected, Kaspersky Industrial CyberSecurity for Nodes uses proxy server settings specified manually. Enter the IP address or symbolic name of the proxy server and the port number
Bypass a proxy server for local addresses	If this functionality is enabled, devices are accessed directly from the network that hosts the protected device with Kaspersky Industrial CyberSecurity for Nodes installed. This option is enabled by default.
Proxy server authentication settings	To authenticate the application on the proxy server for internet access, you must enter the credentials of the user. Kaspersky Industrial CyberSecurity for Nodes supports automatic authentication on the proxy server. If automatic authentication failed, the application prompts you to enter the credentials. **Do not use authentication**. **NTLM authentication**. NTLM authentication with the current user account (default). **NTLM authentication with user name and password**. NTLM authentication with manually specified credentials. **User name and password**. Authentication with manually specified credentials. **Kerberos authentication**. Kerberos authentication with the current user account. To ensure the Kerberos authentication works correctly when using CNAME records for the proxy server address, you must register a Service Principal Name (SPN) for each CNAME record. **Kerberos authentication with user name and password**. Kerberos authentication with manually specified credentials. If Kerberos authentication is selected, Kaspersky Industrial CyberSecurity for Nodes can, depending on the proxy server settings, perform authentication using either the Kerberos or NTLM protocol.
Monitor all network ports	In this network port monitoring mode the protection components monitor data streams that are transmitted via any open network ports of the computer.
Monitor selected network ports only	In this network port monitoring mode, the protection components monitor the selected ports of the computer and the network activity of the selected applications. The list of network ports that are normally used for transmission of email and network traffic is configured according to the recommendations of Kaspersky experts.
Use Kaspersky Security Center as a proxy server when activating the application	Indicate whether Kaspersky Security Center will be used as a proxy-server for application activation.

Configuring scheduled start of local tasks in Web Plug-in

You can use policies to allow or block the start of the local system On-Demand Scan task and the Update task. This is done according to the schedule configured locally on each protected device in the administration group:

- If the scheduled start of a specific type of local system task is prohibited by a policy, these tasks will not be performed on the protected device according to the schedule. You can start local system tasks manually.
- If the scheduled start of a specific type of local system task is allowed by a policy, these tasks will be performed in accordance with the scheduled parameters configured locally for this task.

By default, starting of local system tasks is prohibited by policy.

We recommend that you do not allow local system tasks to start if updates or on-demand scans are administered by Kaspersky Security Center group tasks.

If you do not use group update or on-demand scan tasks, allow local system tasks to be started in the policy: Kaspersky Industrial CyberSecurity for Nodes will perform application database and module updates, and start all local system on-demand scan tasks in accordance with the default schedule.

You can use policies to allow or block the scheduled start of the following local system tasks:

- On-Demand Scan tasks: *Critical Areas Scan*, *Scan at Operating System Startup*, *Application Integrity Control*, *Baseline System Integrity Monitor*.
- The *Update* task.

If the protected device is excluded from the administration group, the local system tasks schedule will be enabled automatically.

To allow or block the scheduled start of Kaspersky Industrial CyberSecurity for Nodes local system tasks in a policy:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application Settings** section.
5. Click **Configure** in the **Run local system tasks** subsection.
6. Configure the settings described in the table below.

Settings for launching local tasks

Parameter	Description
Allow use of local tasks	If the check box is selected, local tasks are displayed in the Kaspersky Industrial CyberSecurity for Nodes local interface. When there are no additional policy restrictions, the user can configure and run tasks. However, configuring task run schedule remains unavailable for the user. The user can run tasks only manually. If the check box is cleared, use of local tasks is stopped. In this mode, local tasks do not run according to schedule. Tasks cannot be started or configured in the local interface of Kaspersky Industrial CyberSecurity for Nodes, or when working with the command line.
Allow schedule management	The check box is available if the **Allow use of local tasks** check box is selected. If the check box is selected, the schedule management becomes available in the local task properties in the Application Console. By default, the check box is cleared.
Allow group tasks to be displayed	If the check box is selected, group tasks are displayed in the Kaspersky Industrial CyberSecurity for Nodes local interface. The user can view the list of all tasks in the Application Console. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes displays an empty task list.
Allow management of group tasks	If the check box is selected, users can start and stop group tasks specified in Kaspersky Security Center. Users can start and stop tasks in the Application Console or in the simplified application interface. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes starts scheduled tasks automatically, or the administrator starts tasks manually in Kaspersky Security Center.

Configuring Quarantine and Backup settings in Web Plug-in

To configure general Quarantine and Backup settings in Kaspersky Security Center:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Supplementary** section.
5. Click the **Settings** button in the **Storages** subsection.
6. Configure the settings described in the table below.

Storage settings

Parameter	Description
On the **Reports** tab, specify the reports settings:	
Store reports no longer than	If the check box is selected, the maximum report storage term is limited to the defined time interval. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file.
Limit the size of report file to	If the check box is selected, the maximum report file size is limited to the defined value. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries from the report file when the maximum report file size is reached.
On the **Backup** tab, specify the Backup settings:	
Store objects no longer than	If the check box is selected, the maximum file storage term is limited to the defined time interval. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Industrial CyberSecurity for Nodes deletes the oldest files from Backup.
Limit the size of Backup to	If the check box is selected, the maximum storage size is limited to the defined value. By default, the maximum size is 400 MB. To avoid exceeding the maximum storage size, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest files from storage when the maximum storage size is reached.

Parameter	Description
Threshold value for available space	The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value is 100 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the Backup free space threshold exceeded event and issues a notification according to the settings for notifications about events of this type. If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the amount of free space in Backup. The **Threshold value for available space** check box is active if the **Limit the size of Backup to** check box is selected. The check box is selected by default.
On the **Quarantine** tab, specify the Quarantine settings:	
Limit the size of Quarantine to	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes monitors the total size of objects placed in Quarantine. If the specified value is exceeded (the default value is 1024 MB), Kaspersky Industrial CyberSecurity for Nodes logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type. Meanwhile the application stops quarantining new objects. You must empty the Quarantine manually. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the total size of objects placed in Quarantine. By default, the functionality is disabled.
Threshold value for available space	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the minimum amount of free space in Backup (the default value is 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Quarantine free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. The **Threshold value for available space** check box is active if the **Limit the size of Quarantine to** check box is selected. This option is enabled by default.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Industrial CyberSecurity for Nodes on several protected devices.

Global Kaspersky Security Center policies can be created for managing protection on several devices where Kaspersky Industrial CyberSecurity for Nodes is installed.

A policy enforces the Kaspersky Industrial CyberSecurity for Nodes settings, functions and specified tasks on all the protected devices for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has *Active* status in the Web Console.

Information on policy enforcement is logged in the Kaspersky Industrial CyberSecurity for Nodes system audit log. This information can be viewed in the Application Console in the **Logs and notifications** node.

Kaspersky Security Center offers one way to apply policies on protected devices: *Prohibit changing the settings*. After a policy has been applied, Kaspersky Industrial CyberSecurity for Nodes uses the settings for which you have selected the icon in the policy properties on protected devices. In this case, the selected settings are used instead of the settings in effect before the policy was applied. Kaspersky Industrial CyberSecurity for Nodes does not apply the active policy settings for which the icon is selected in the policy properties.

If a policy is active, the values of settings marked with the icon in the policy are displayed in the Application Console but cannot be edited. The values of other settings (marked with the icon in the policy) can be edited in the Application Console.

The settings configured in the active policy and marked with the icon also block changes in Kaspersky Security Center for an individual protected device in the **Properties: <Protected device name>** window.

Settings that are specified and sent to the protected device using an active policy are saved in the local task settings after the active policy is disabled.

If a policy defines settings for any real-time computer protection task or network storage protection task that is currently running, the settings defined by the policy will change immediately after the policy is applied. If the task is not running, the settings are applied when it starts.

How to create a policy in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click **Add**.
3. The **New policy** window opens.
4. In the **Select application** section, select Kaspersky Industrial CyberSecurity for Nodes.
5. Specify the modes of Kaspersky Industrial CyberSecurity for Nodes on protected devices.
6. If necessary, specify files or folders as well as names of objects (according to the Virus Encyclopedia) that you want to exclude from scanning by all or some application components.
7. On the **General** tab, you can perform the following actions:
   - Change the policy name.

     The policy name cannot contain the following symbols: `" * < : > ? \ | .`

   - Select the policy status:
     - **Active**. After the next synchronization, the policy will be used as the active policy on the computer.
     - **Inactive**. Backup policy. If necessary, an inactive policy can be switched to active status.
     - **Out-of-office**. The policy is activated when a computer leaves the organization network perimeter.
   - Configure the inheritance of settings:
     - **Inherit settings from parent policy**. If this toggle button is switched on, the policy setting values are inherited from the top-level policy. Policy settings cannot be edited if is set for the parent policy.
     - **Force inheritance of settings in child policies**. If the toggle button is on, the values of the policy settings are propagated to the child policies. In the child policy settings the **Inherit settings from parent policy** check box is automatically selected. Child policy settings are inherited from the parent policy, except for the settings marked with . Child policy settings cannot be edited if is set for the parent policy.
8. On the **Application settings** tab, configure the policy settings as required.
9. Click **Save**.

After a new policy is created, a set of allowing rules is created to prevent applications from being blocked, ensuring their uninterrupted operation.

By default, Kaspersky Industrial CyberSecurity for Nodes creates a set of rules for inbound network traffic when creating a new policy:

- Two allowing rules for the process of sharing the Windows desktop using Kaspersky Security Center Network Agent, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 15000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

By default, Kaspersky Industrial CyberSecurity for Nodes creates a set of outgoing network traffic rules when creating a new policy:

- Two allowing rules for the Kaspersky Industrial CyberSecurity for Nodes service, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for the worker process of Kaspersky Industrial CyberSecurity for Nodes, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 13000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Industrial CyberSecurity for Nodes tasks, and how to create them, configure task settings, and start and stop them.

About task creation in Web Plug-in

You can create local and group tasks in the following ways:

- For one protected device: in the **Properties <Protected device name>** window in the **Tasks** section.
- For an administration group: in the details pane of the node of the selected group of protected devices on the **Tasks** tab.
- For a set of protected devices: in the details pane of the **Device selections** node.

You can use policies to disable schedules for *Update* and *On-Demand Scan* local system tasks on all protected devices in the same administration group.

General information on tasks in Kaspersky Security Center is provided in the Kaspersky Security Center Help.

Creating a task in Web Plug-in

To create a new task in the Kaspersky Security Center Web Console:

1. Start the task wizard in one of the following ways:

   - To create a local task:

     a. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

     b. Click the protected device name.

     c. In the **<Device name>** window that opens, select the **Tasks** tab.

     d. Click **Add**.

   - To create a group task:

     a. In the main window of the Web Console, select **Asset management** → **Tasks**.

     b. Click **Add**.

   The task wizard window opens.

2. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.

3. In the **Task type** drop-down list, select the type of the task to be created.

4. Depending on the selected task type, do one of the following:

   - Create an On-Demand Scan task.

   - To create an update task, configure task settings based on your requirements:

     a. You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source in the **Update sources** block. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.

     You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

     b. Configure the settings for a feature that reduces the load on the disk subsystem:

     c. You can specify the actions that Kaspersky Industrial CyberSecurity for Nodes will perform if critical application module updates are needed, as well as after installation of critical updates is complete. In addition, you can specify whether Kaspersky Industrial CyberSecurity for Nodes will receive information about available scheduled updates.

     d. Specify the set of updates to copy and a path to the folder that will be used by Kaspersky Industrial CyberSecurity for Nodes to store copied updates.

- To create the Application Activation task:

  a. In the **Selecting a license key** window, specify the key file or activation code that you want to use to activate the application.

  b. Select the **Use as a reserve key** check box if you want to create a task for renewing the license.

- Create and configure the Rule Generator for Applications Launch Control task.

- Create and configure the Rule Generator for Device Control task.

5. Click **Next**.

6. If the task is being created for a set of protected devices, select the network (or group) of protected devices on which this task will be executed.

7. Click **Next**.

8. In the **Finish task creation** window, select the **Open task details when creation is complete** check box if you want to configure task settings.

9. Click **Finish**.

The created task is displayed in the **Tasks** list.

Configuring group tasks in Web Plug-in

To configure a group task for multiple protected devices:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. Go to the **Application settings** tab.

4. Depending on the type of configured task, do one of the following:

   - To configure the *On-Demand Scan* task:

     a. In the **Scan scope** section, configure a scan scope.

     b. In the **Options** section, configure the level of heuristic analysis and integration with other application components.

   - To configure the *Update* task, adjust the task settings based on your requirements:

     a. In the **Update sources** section, configure update source settings.

     b. In the **Update settings** section, manage the disk subsystem optimization settings, specify the actions that you want Kaspersky Industrial CyberSecurity for Nodes to perform if critical updates of application modules are available or if information about planned updates is available; specify the update copying settings.

- To configure the *Application Activation* task, apply the key file or activation code that you want to use to activate the application. Select the **Use as additional key** check box if you want to add an activation code or key file for renewing the license.

- To configure the automatic generation of allowing rules for Device Control, specify the settings that will be used to create the list of allowing rules.

5. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except *Update rollback*).

6. On the **Settings** tab in the **Account** section, specify the account whose rights will be used to run the task. For detailed information on configuring settings in this section, see Kaspersky Security Center Help.

7. Click **Save**.

The newly configured group task settings are saved.

Configuring the Application activation task in Web Plug-in

To configure the Application Activation task:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. In the **Application settings** section, specify the key file that you want to use to activate the application. Select the **Use as a reserve key** check box if you want to add a key to renew the license.

4. Configure the task schedule in the **Schedule** section.

5. Click the **Save** button in the **<Task name>** window.

Configuring the Update task in Web Plug-in

To configure the Update task:

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

2. Click the task name in the list of Kaspersky Security Center tasks.

   The <Task name> window opens.

3. Select the **Application settings** tab.

4. In the **Update sources** section, configure update source settings:

   a. Specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually, and setting them as update sources.

      You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

b. Configure the settings for a feature that reduces the load on the disk subsystem:

- **Lower the load on the disk I/O**
- **RAM used for optimization, MB**

c. Specify actions that Kaspersky Industrial CyberSecurity for Nodes should perform when critical updates of application modules are available or when there is information about planned updates.

d. Specify update copying settings.

5. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except *Update rollback*).

6. In the **<Task name>** window, click **OK**.

Scheduling tasks

You can schedule local system and custom tasks in the Web Console.

To schedule group tasks using the Web Console:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. Go to the **Schedule** section and configure the schedule settings (see the table below) as needed.

   Fields with schedule settings for the On-Demand Scan and Update tasks are unavailable if scheduling of these tasks is blocked by a Kaspersky Security Center policy.

4. Click the **Save** button to save the task start settings.

Task schedule settings

Parameter	Description
Scheduled start	Select the task run mode: • **Every N hours**. The task will run periodically every few hours. Specify the start time of the task and the period in hours. • **Every N days**. The task will run periodically every few days. Specify the start time of the task and the period in days. • **Every N minutes**. The task will run periodically every few minutes. Specify the start time of the task and the period in minutes. • **By days of week**. The task will run on the specified days of the week. Select the days of the week and specify the start time. If you need to run the task at intervals of several weeks, enter the desired value in the **Interval** field. • **Monthly**. The task will run on a certain day of the month. Specify the date and time of the start. • **Once**. The task will run once at the specified date and time. • **Manually**. Run mode in which you can start scan manually at a time when it is convenient for you. • **When new updates are downloaded to the repository**. The task will run every time updates are downloaded to the repository. • **On completing another task**. The task will run upon completion of another task. Select the task and its completion status. Kaspersky Industrial CyberSecurity for Nodes does not support the **On completing another task** mode for scheduling local tasks. • **On virus outbreak**. The task will run if a virus attack is detected. • **Start in N minutes after application startup**. The task will run after a specified period of time every time Kaspersky Industrial CyberSecurity for Nodes starts. Specify the number of minutes in the **Task start delay (min)** field.
Run missed tasks	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes starts the skipped task as soon as it becomes possible. The task may be skipped, for example, if the computer was off at the scheduled task start time. When the application gets an opportunity to execute missed tasks, it runs the tasks randomly within a certain time interval to distribute the load on the computer. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes does not run skipped tasks. Instead, it carries out the next task in accordance with the current schedule.
Use automatically randomized delay for task starts	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Use automatically randomized delay for task starts within an interval of	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Turn on devices by using the Wake-on-LAN function before starting the task	If the check box is selected, the operating system of the computer is given a specified lead time to complete startup before the task is run. The default lead time is 5 minutes. Select the check box if you want to run the task on all computers including powered off computers.
Shut down the devices after completing the task	If this check box is selected, the computer will shut down after the task is completed. For example, you can enable this functionality to scan the computer on Fridays after working hours. When the task finishes, the application turns off the computer for the weekend.
Stop the task if it runs longer than	Limiting the task execution time. After the specified amount of time, Kaspersky Industrial CyberSecurity for Nodes stops the task. The task is not marked as completed. Next time Kaspersky Industrial CyberSecurity for Nodes runs the task, it will be run from the beginning and on schedule.

Parameter	Description
Pause task execution	You can specify a time interval during which the execution of a previously scheduled task will be paused. Once the specified time period is over, the task will resume. This may be necessary, for example, to minimize the impact of Kaspersky Industrial CyberSecurity for Nodes on the performance of your computer during periods of peak usage. This functionality is available only for On-Demand Scan tasks.
End date	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes will stop running the scheduled task starting on the specified date. The task will be set to **Manually** mode. This functionality is available only for On-Demand Scan tasks.

Reports in Kaspersky Security Center

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are based on information stored on Administration Server.

Starting from Kaspersky Security Center 11, the following types of reports are available for Kaspersky Industrial CyberSecurity for Nodes:

- Report on the status of application components
- Report on prohibited applications
- Report on prohibited applications in test mode

See Kaspersky Security Center Help for detailed information about all Kaspersky Security Center reports and how to configure them.

Report on the status of Kaspersky Industrial CyberSecurity for Nodes components

You can monitor the protection status of all network devices and get a structured overview of the set of components on each device.

The report displays one of the following states for each component: *Running*, *Paused*, *Stopped*, *Not covered by license*.

Not Installed status refers to the component, not the application itself. If the application is not installed, the Kaspersky Security Center Web Console assigns the N/A (Not available) status.

You can create component selections and use filtering to display network devices with a specified set of components and state.

See Kaspersky Security Center Help for detailed information about creating and using selections.

To view the status of components in the Kaspersky Security Center Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed Devices**.
2. Click the device name and go to the **Applications** section.
3. Click the application name of Kaspersky Industrial CyberSecurity for Nodes.
4. In the window that opens, on the **General** tab, go to the **Components** section.
5. Review the status table.

To review a standard report in Kaspersky Security Center Web Console:

1. Select **Monitoring** → **Reports**.
2. In the list, select **Report on status of application components** and click it.

   A report is generated.
3. Review the following report details:

   - A graphical diagram.
   - A summary table of components and aggregated numbers of network devices where each of the components is installed, and groups they belong to.
   - A detailed table specifying the component status, version, device and group.

Reports on prohibited applications in active and test modes

Based on the results of the Applications Launch Control task, two types of reports can be generated: a report on prohibited applications (if the task is started in Active mode) and a report on prohibited applications in test mode (if the task is started in the Inform mode). These reports display information about blocked applications on the protected devices of the network. Each report is generated for all administration groups and accumulates data from all the Kaspersky applications installed on the protected devices.

To review a report on prohibited applications in the Inform mode:

1. Run the Applications Launch Control task in Inform mode.
2. Select **Monitoring** → **Reports**.
3. In the list, select **Report on prohibited applications in test mode** and click it.

   A report is generated.

4. Review the following report details:

   - A graphical diagram that displays the top 10 applications with the largest number of blocked starts.
   - A summary table of application blocks, specifying the executable file name, reason, time of blocking, and number of devices where the blocking occurred.
   - A detailed table specifying data about the device, file path and criteria for blocking.

To review a report on prohibited applications in Active mode:

1. Run the Applications Launch Control task in Active mode.
2. Select **Monitoring → Reports**.
3. In the list, select **Report on prohibited applications** and click it.

   A report is generated.

This report consists of the same data about blocks as the report on prohibited applications in test mode.

Application licensing

This section provides information about the main concepts related to licensing of the application.

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 review the terms of the End User License Agreement before you start using the application.

You can read the terms of the End User License Agreement and the Privacy Policy, that describes processing and transmission of data, in the following ways:

- During the installation of Kaspersky Industrial CyberSecurity for Nodes.
- During the installation of Kaspersky Industrial CyberSecurity for Nodes Console.
- During the installation of Kaspersky Security Gateway.
- By reading the file license.txt document included in the distribution kit.
- On the Kaspersky web site (https://www.kaspersky.com/business/eula).

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

About the license

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A valid license entitles you to receive use of the application in accordance with the terms of the End User License Agreement as well as receive technical support when necessary.

The scope of service and the period of application use depend on the type of license used to activate the application.

You can activate the application in two ways:

- Using a key file, which grants you the usage under the commercial license
- Using an activation code to purchase a commercial license.

After the commercial license expires, only the following application components and tasks remain available without database updates:

- Real-Time File Protection
- System Integrity Monitoring
- On-Demand Scan tasks

To continue using all the features of Kaspersky Industrial CyberSecurity for Nodes, you must renew your commercial license. It is recommended to extend the validity period of the license before its expiration date to ensure maximum protection.

If the license key is removed, the application will continue to run. The System Integrity Monitoring component remains available, and the rest of components, tasks, and Kaspersky Industrial CyberSecurity for Nodes database updates become unavailable. The same happens if Kaspersky adds your license to the denylist.

About license certificate

A *license certificate* is a document transferred to the user together with a key file or activation code.

The license certificate contains the following license information:

- License ID or order number.
- Details of the user to whom the license is granted.
- Details of the application that can be activated using the license.
- Limitation on the number of licensed units (for example, the number of devices on which the application can be used under the license).
- License term start date.
- License expiration date or license term.
- License type.

About the key

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky.

You can add a key to the application by using a key file or an activation code. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky can add a key to the denylist due to violations of the License Agreement. If your key is blocked, a different key must be added in order for the application to work.

There are two types of keys: active and reserve.

An *active key* is a key that is currently used by the application. A key for a commercial license may be added as the active key. The application cannot have more than one active key.

A *reserve key* is a key that entitles the user to use the application, but is not currently in use. A reserve key automatically becomes active when the license associated with the current active key expires. A reserve key can be added only if the active key is available.

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky. The purpose of a key file is to add a license key that activates the application.

You receive a key file at the email address you specified after purchasing Kaspersky Industrial CyberSecurity for Nodes.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can recover a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To recover a key file, do one of the following:

- Contact the license seller.
- Obtain a key file on the Kaspersky website based on your existing activation code.

About activation code

An *activation code* is a unique sequence of 20 letters and numbers. You have to enter an activation code in order to add a key for activating Kaspersky Industrial CyberSecurity for Nodes. You receive an activation code at the email address you specified after purchasing Kaspersky Industrial CyberSecurity for Nodes.

To activate the application with an activation code, Internet access is required to connect to Kaspersky activation servers.

If you have lost your activation code after installing the application, it can be recovered. You may need the activation code to register a Kaspersky CompanyAccount, for example. To recover your activation code, contact the Kaspersky Lab partner from whom you purchased the license.

Activating the application with a key file

You can activate Kaspersky Industrial CyberSecurity for Nodes by applying a key file.

To activate Kaspersky Industrial CyberSecurity for Nodes by applying a key file:

1. In the Application Console tree, expand the **Licensing** node.
2. Click the **Add key** link in the results pane of the **Licensing** node.

3. In the window that opens, click the **Browse** button.
4. Select a key file with the .key extension.

   You can also add a key as a reserve key. To add a key as an additional key, select the **Use as additional key** check box.

5. Click **OK**.

The selected key file will be applied. In this case:

- If an active key has already been added to activate the application and you add another key as the active key, the new key replaces the previously added key. The previously added key is removed.
- If a reserve key has already been added to activate the application and you add another key as a reserve key, the new key replaces the previously added key. The previously added reserve key is removed.
- If an active key and a reserve key have already been added to activate the application and you add a new key as the active key, the new key replaces the previously added active key; the reserve key is not removed.

Information about the added key will be available on the **Licensing** node.

Activating the application with an activation code

To activate the application using an activation code, the protected device must be connected to the internet.

You can activate Kaspersky Industrial CyberSecurity for Nodes by using an activation code.

When activating the application with this method, Kaspersky Industrial CyberSecurity for Nodes sends data to the activation server to verify the entered code:

- If the activation code verification is successful, the application is activated.
- If the activation code verification fails, the corresponding notification is displayed. In this case, you must contact the software vendor from whom you purchased your Kaspersky Industrial CyberSecurity for Nodes license.
- If the number of activations with the activation code is exceeded, the corresponding notification is displayed. The application activation procedure is interrupted, and the application prompts you to contact Technical Support.

You can activate Kaspersky Industrial CyberSecurity for Nodes with an activation code using the Application Console, or by creating the *Application Activation* group task via the Administration Plug-in or via the Web Plug-in.

To activate Kaspersky Industrial CyberSecurity for Nodes with an activation code using the Application Console:

1. In the Application Console tree, expand the **Licensing** node.
2. Click the **Add activation code** link in the results pane of the **Licensing** node.

3. In the window that opens, enter the activation code in the **Activation code** field.

   - If you want to use the activation code as a reserve key, select the **Use as additional key** check box.
   - To view information about a license, click the **Show license information** button. The information will be displayed in the **License information** block.

4. Click **OK**.

   Kaspersky Industrial CyberSecurity for Nodes sends information about the applied activation code to the activation server.

Viewing information about current license

Viewing the license status

Information about the status of the current license is displayed in the details pane of the **Kaspersky Industrial CyberSecurity for Nodes** node of the Application Console. License status can have the following values:

- **Checking the key status** – Kaspersky Industrial CyberSecurity for Nodes is checking the added key file and is waiting for a response about the current status.
- **Expiration date** – Kaspersky Industrial CyberSecurity for Nodes has been activated until the specified date. The status is highlighted in yellow in the following cases:
  - The license will expire in 30 days and no reserve key have been added.
  - The added key has been added to the denylist and is about to be blocked.
- **Application is not activated** – Kaspersky Industrial CyberSecurity for Nodes is not activated because the key has not been added. The status is highlighted in red.
- **License has expired** – Kaspersky Industrial CyberSecurity for Nodes is not activated because the license has expired. The status is highlighted in red.
- **End User License Agreement has been violated** – Kaspersky Industrial CyberSecurity for Nodes is not activated because the terms of the End User License Agreement have been violated. The status is highlighted in red.
- **Key is in denylist** – the added key file has been blocked and added to the denylist by Kaspersky, for example, if the key was used by third parties to activate the application illegally. The status is highlighted in red.

Viewing information about current license

To view the information about the current license,

In the Application Console tree, expand the **Licensing** node.

General information about the current license is displayed in the details pane of the **Licensing** node (see the table below).

General information about the license in the Licensing node

Field	Description
Activation code status or key status	Activation code status or key status: *Active key* or *Reserve*.
Expiration date	Expiry date and time of the license associated with an active key.
License type	License type: *Commercial license*.
Activation status	The activation status information can take the following values: • **Applied** – if you have activated the application using a key. • **Application Activation** – if you have applied an activation code to activate the application, but the activation process has not been finalized yet. The status changes to **Applied** after activation of the application is complete and the contents of the node's details pane are refreshed. • **Activation error** – if application activation failed. You can view the cause of unsuccessful activation in the task log.
Key	The number of the key that you used to activate the application.

To view the detailed information about license,

in the details pane of the **Licensing** node open the context menu of the license you want view and select **Properties**.

Detailed license information in the Properties <Key number> window

Field	Description
Key	The number of the key that you used to activate the application.
Application	The name of the application that was activated with the added key.
License type	License type: commercial or trial.
License term	The number of days, starting from the application activation date, during which the license is valid.
Activation date	Date when the key was added to the application.
Expiration date	Expiry date of the license associated with an active key. If you activate the application under unlimited subscription, the field value is *Unlimited*. If Kaspersky Industrial CyberSecurity for Nodes is unable to determine the license expiry date, the field value is set to *Unknown*.
Days till expiration	Number of days remaining until the expiry of the license associated with the active key.
Eligible for technical support	Information on whether Kaspersky or its partners will provide technical support for customers according to the license terms.
Support information	Contact details of Kaspersky or of its partner providing technical support. This field may be empty if technical support is not provided.
Owner information	Information about the license customer: a customer name and the name of an organization for which the license was acquired.
License information	Number and type of current license.
Functionality	Application features that are available under the license.

Renewing license

By default, Kaspersky Industrial CyberSecurity for Nodes notifies you when the license has 30 days remaining before expiration.

You can renew the license before the expiration date using a reserve key. This ensures that your device remains protected after expiration of the current license and before you activate the application with a new license.

To renew a license:

1. Obtain a new activation code or a key file.
2. In the Application Console tree, select the **Licensing** node.
3. Perform one of the following actions in the results pane of the **Licensing** node:
   - If you want to renew a license using a key file:
     a. Click the **Add key** link.
     b. In the window that opens, click the **Browse** button.
     c. Select a new key file with the .key extension.
     d. Select the **Use as additional key** check box.
   - If you want to renew a license using an activation code:
     a. Click the **Add activation code** link.
     b. Enter the purchased activation code in the window that opens.
     c. Select the **Use as additional key** check box.

     An Internet connection is required to apply an activation code.
4. Click **OK**.

The reserve key will be added and automatically applied upon expiration of the current Kaspersky Industrial CyberSecurity for Nodes license.

Deleting the key

If you delete an added key, you can restore it by re-applying the key file.

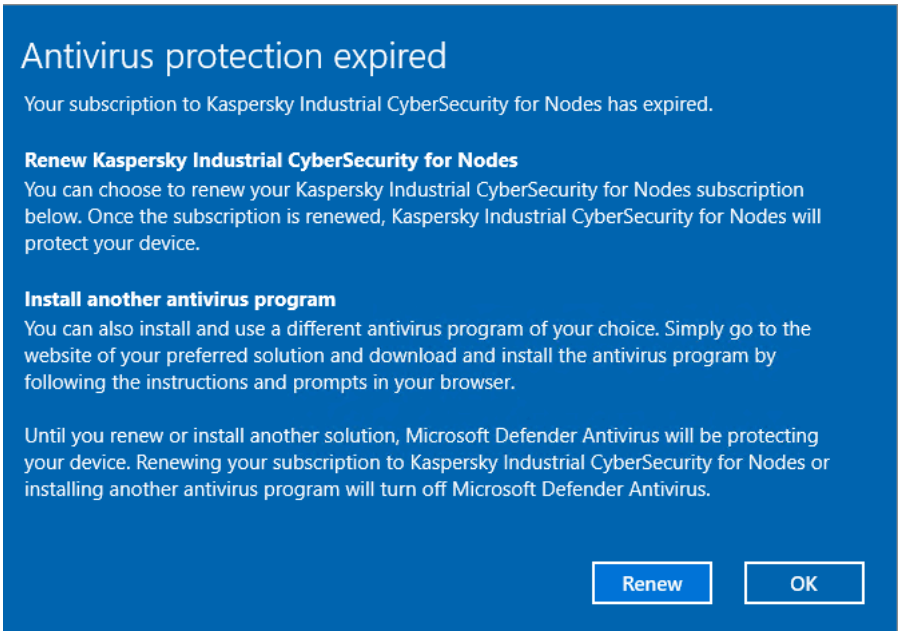
To remove the previously added key:

1. In the Application Console tree, select the **Licensing** node.
2. In the results pane of the **Licensing** node in the table containing information on added keys, select the key that you want to remove.
3. In the context menu of the line containing information on the selected key, select **Remove**.
4. Click the **Yes** button in the confirmation window to confirm that you want to delete the key.

The selected key will be removed.

After the key is removed, the computer is no longer protected by Kaspersky Industrial CyberSecurity for Nodes. The application then sends a protection status command to the Windows Security Center (WSC) to enable built-in protection tools. While doing so, the application displays a window suggesting to renew the license (see the figure below). If the pop-up window hinders other applications and you want to disable this window, in the Registry, set `NeedShowUPAOWindows=0`. This key is under `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment\`.

If you disable the license renewal window, Kaspersky Industrial CyberSecurity for Nodes does not send the protection status command to the Windows Security Center. This means that the Windows Security Center does not enable the built-in protection tools. Keep this risk in mind when disabling the window.



Window suggesting license renewal

Starting and stopping Kaspersky Industrial CyberSecurity for Nodes

This section contains information about starting and stopping Kaspersky Industrial CyberSecurity for Nodes, as well as about starting Kaspersky Industrial CyberSecurity for Nodes Console and Management Plug-in for the Kaspersky Security Center Administration Console.

Starting and stopping the application

After installing Kaspersky Industrial CyberSecurity for Nodes to a user's computer, the application is started automatically. By default, Kaspersky Industrial CyberSecurity for Nodes is started after operating system startup. It is not possible to configure automatic startup of the application in the operating system settings.

Downloading Kaspersky Industrial CyberSecurity for Nodes anti-virus databases after the operating system starts can take up to two minutes depending on the capabilities of the computer. During this time, the level of computer protection is reduced. The downloading of anti-virus databases when Kaspersky Industrial CyberSecurity for Nodes is started on an already started operating system does not cause a reduction in the level of computer protection.

How to configure the automatic application startup in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Application settings** → **Security and reliability** and click **Settings**.
4. On the **Security** tab, select or clear the **Start the application on computer startup (recommended)** check box to enable or disable autorun for the application.
5. Save your changes.

How to configure the automatic application startup in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Application Settings** → **Security and reliability**.
5. Click **Configure**.

   The **Security and reliability** window opens.

6. Use the **Start the application on computer startup (recommended)** check box to enable or disable automatic application startup.

7. Save your changes.

How to configure the automatic application startup in the Application Console

1. select the **Kaspersky Industrial CyberSecurity for Nodes** node in the Application Console tree.

2. Select **Application properties** in the node's context menu.

3. This opens a window; in that window, select the **Security settings** tab.

4. Use the **Start the application on computer startup (recommended)** check box to enable or disable automatic application startup.

5. Save your changes.

You can start and stop Kaspersky Industrial CyberSecurity for Nodes if you are a member of the Administrators group on the protected device.

How to start or stop the application in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.

2. In the workspace, select the **Devices** tab.

3. Double-click to open the computer properties window.

4. In the computer properties window, select the **Applications** section.

5. In the list of Kaspersky applications installed on the computer, select **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

6. Do one of the following:

   - To start the application, click the button to the right of the list of Kaspersky applications.
   - To stop the application, click the button to the right of the list of Kaspersky applications.

How to start or stop the application in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.

2. Click the name of the computer on which you want to start or stop Kaspersky Industrial CyberSecurity for Nodes.

   The computer properties window opens.

3. Select the **Applications** tab.

4. Select the check box opposite **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

5. Click the **Start** or **Stop** button.

How to start or stop the application in the Application Console

1. To stop Kaspersky Industrial CyberSecurity for Nodes:

   a. Open the Application Console.

   > The user account must have permissions to access the **Exit the application** functionality.

   b. In the Application Console tree, open the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.

   c. Select **Stop application**.

   d. In the confirmation window, click the **Yes** button to confirm stopping the application.

   The application will be stopped.

2. To start **Kaspersky Industrial CyberSecurity for Nodes**:

   a. Run the avpui.exe file in the Application Console installation folder on the protected device. By default, the file is located in the C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console folder.

   The **Select protected device** window opens.

   b. If Kaspersky Industrial CyberSecurity for Nodes and the Application Console are installed on the same computer, select **Local computer (the computer on which the Application Console is running)**.

   c. If Kaspersky Industrial CyberSecurity for Nodes and the Application Console are installed on different computers:

      1. Select **Another device**.

      2. Click **Browse** and specify the name of the computer where the application is installed.

      3. Specify the port for connecting to the computer with the installed application:

         - **Using Windows credentials**. A port for connecting with Windows credentials. The default value is 13032.

         - **Using credentials from manually created users**. A port for connecting manually created users with credentials. The default value is 13031.

   d. If necessary, enable the **Use authentication** functionality and enter the credentials to connect the Application Console to the computer where the application is installed. The specified user account must have permissions to access the **Read settings** and **Remote connection to application** functionalities on the computer where the application is installed.

   e. Click **Application management service**.

   f. In the window that opens, click the **Start** button.

   The application will be started.

The **Select protected device** window is also displayed if the connection to the computer on which the application is installed is lost or if the KICS service fails. You can restore the KICS service by clicking the **Start** button.

You can also start or stop the application on the command line.

Pausing and resuming computer protection and control

Pausing computer protection and control means disabling all protection and control components of Kaspersky Industrial CyberSecurity for Nodes for some time.

The application status is displayed using the application icon in the taskbar notification area.

- The icon signifies that computer protection and control are paused.
- The icon signifies that computer protection and control are enabled.

Pausing or resuming computer protection and control does not affect scan or update tasks.

If any network connections are already established when you pause or resume computer protection and control, a notification about the termination of these network connections is displayed.

To pause computer protection and control:

1. In the Application Console tree, open the context menu of the **Kaspersky Industrial CyberSecurity for Nodes** node.
2. Select **Pause protection**.
3. Select one of the following options:
   - **Pause for the specified time <time period>** – computer protection and control will resume after the amount of time that is specified in the drop-down list below.
   - **Pause until restart** – computer protection and control will resume after you restart the application or restart the operating system. Automatic startup of the application must be enabled to use this option.
   - **Pause** – computer protection and control will resume when you decide to re-enable them.

   Kaspersky Industrial CyberSecurity for Nodes will pause the operation of all protection and control components that are not marked by a lock () in the policy.

To resume computer protection and control:

1. Open the context menu of the application icon, located in the taskbar notification area.
2. In the context menu, select **Resume protection**.

You can resume computer protection and control at any time, regardless of the computer protection and control pause option that you selected previously.

Compact Diagnostic Interface

This section describes the use of Compact Diagnostic Interface.

About the Compact Diagnostic Interface

The Compact Diagnostic Interface component is installed and uninstalled along with the System Tray Icon component independently from the Application Console, and can be used when the Application Console is not installed on the protected device. The Compact Diagnostic Interface is started from the System Tray Icon or by running avpui.exe from the application folder on the protected device.

In the Compact Diagnostic Interface, you can do the following:

- Open the **About** window with the list of installed updates and available patches.
- Review information about the general application status.
- Review security incidents that have occurred.
- Review current activity on the protected device.
- Start or stop writing dump and trace files.
- Create Portable Auditor.
- Open the Application Console.

The Compact Diagnostic Interface is available even if access to Kaspersky Industrial CyberSecurity for Nodes functions is password-protected. No password is required.

> The Compact Diagnostic Interface component cannot be configured via Kaspersky Security Center.

Reviewing the Kaspersky Industrial CyberSecurity for Nodes status via the Compact Diagnostic Interface

To view the application status using the Compact Diagnostic Interface:

1. Open the Compact Diagnostic Interface in one of the following ways:
   - Run the avpui.exe file in the application installation folder on the protected device. By default, the file is located in C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.
   - Click the application icon in the taskbar notification area.

2. Review the current status of the key, Real-Time Computer Protection tasks, and Update tasks in the **Protection status** section. Different colors are used to notify the user about the protection status (see the table below).

Color indication in the Compact Diagnostic Interface window

Section	Status
Real-time protection status	The panel is *green* if the following conditions are met: • The Real-Time File Protection component is enabled. • The Applications Launch Control component is running in **Block** mode.
	The panel is *yellow* if one or more of the following conditions are met: • The Real-Time File Protection component is disabled. • The Applications Launch Control component is running in **Inform** mode.
	The panel is *red* if both of the following conditions are met: • The Real-Time File Protection component is disabled or not installed. • The Applications Launch Control component is not installed or is running in **Inform** mode.
Licensing	The panel is *green* if the current license is valid.
	A *yellow* panel signifies that one of the following events has occurred: • *Checking the license status.* • *The license will expire in 14 days and no additional key or activation code has been added.* • *The added key has been added to the denylist and is about to be blocked.*
	A *red* panel signifies that one of the following events has occurred: • *Application is not activated.* • *License has expired.* • *End User License Agreement has been violated.* • *Key is in denylist.*
Update	The panel is *green* when Application databases are up-to-date.
	The panel is *yellow* when Application databases are out of date.
	The panel is *red* when Application databases are extremely out of date.

Reviewing security event statistics

The **Statistics** section displays all security events. Each protection task statistic is displayed in a separate block specifying the number of incidents and the date, and time when the last incident occurred. When an incident is logged, the block color changes to red.

To view the statistics:

1. Open the Compact Diagnostic Interface in one of the following ways:

   - Run the avpui.exe file in the application installation folder on the protected device. By default, the file is located in C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.

   - Click the application icon in the taskbar notification area.

2. Go to the **Statistics** section.

3. Review the security incidents for the protection tasks.

Reviewing current application activity

To review the current application activity on the protected device:

1. Open the Compact Diagnostic Interface in one of the following ways:
   - Run the avpui.exe file in the application installation folder on the protected device. By default, the file is located in C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.
   - Click the application icon in the taskbar notification area.
2. Go to the **Current application activity** section.

Different colors are used to indicate the application activity status:

- In the **Tasks** section:
  - *Green*. There are no conditions that would require yellow or red.
  - *Yellow*. Critical areas have not been scanned for a long time.
  - *Red*. At least one of the following conditions is true:
    - No tasks are started and a start schedule is not set up for any of the tasks.
    - Application launch errors are logged as critical events.
- In the **Kaspersky Security Network** section:
  - *Green*. The **KSN Usage** task is started.
  - *Yellow*. The KSN Statement is accepted, but the task is not started.

Configuring application tracing and memory dump recording

To configure application tracing and memory dump recording:

1. Open the Compact Diagnostic Interface in one of the following ways:
   - Run the avpui.exe file in the application installation folder on the protected device. By default, the file is located in C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.
   - Click the application icon in the taskbar notification area.
2. Go to the **Malfunction diagnosis** section.
3. Use the **Enable dump and trace files protection** check box to enable or disable protection of dump files and trace files.

If protection of dump files and trace files is enabled, the files can be accessed by the following users:

- Dump files can be accessed by the system administrator and local administrator, and by the user that enabled the writing of dump files and trace files.
- Trace files can be accessed only by the system administrator and local administrator.

4. Use the **Write debug information to trace file** check box to enable or disable tracing of application operation.

   By default, application operation tracing is disabled.

5. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, click the **Browse** button and select the required folder.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

   In the selected folder, Kaspersky Industrial CyberSecurity for Nodes creates a subfolder named logs-Kaspersky Industrial CyberSecurity for Nodes-<uid> to store trace files, where <uid> is a unique 8-character log identifier.

6. Select the level of detail of debug information:

   - **Normal** means the trace file saves messages about all errors, warnings, as well as information about normal operation of the application (default).
   - **Critical** means the trace file saves only messages about fatal errors.
   - **Diagnostic** means the trace file saves messages about all errors as well as warnings.
   - **Important** means the trace file saves messages about all errors, warnings, and additional information.
   - **Detailed** means the trace file saves all information about the operation of the application.

   A Technical Support representative determines the detail level required to resolve any potential issues.

7. To delete old trace files, enable the **Remove the oldest trace files** functionality.

   If this functionality is enabled, configure the maximum size and number of trace files:

   a. Specify the **Maximum size of a trace file (MB)**.

      Available values: from 1 to 4095 MB. The default value is 100 MB.

   b. Specify the **Maximum number of trace files**.

      Available values: from 1 to 999. The default value is 5.

8. Use the **Create a dump file on malfunction to the folder** check box to enable or disable tracing of application operation.

   By default, memory dump recording is disabled.

9. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, click the **Browse** button and select the required folder.

   The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

10. Click **Apply**.

Kaspersky Industrial CyberSecurity for Nodes self-defense

Self-Defense prevents other applications from performing actions that can interfere with the operation of Kaspersky Industrial CyberSecurity for Nodes. The application has self-defense mechanisms that protect the application against modification or deletion of its folders, memory processes, and system registry entries. Kaspersky Industrial CyberSecurity for Nodes supports the Antimalware Protected Process Light (AM-PPL) technology by Microsoft, which protects application processes from malicious activity. Additionally, the application allows managing user access permissions to application functionality and separately to the application service.

Enabling and disabling Self-Defense

Kaspersky Industrial CyberSecurity for Nodes prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

The technology blocks access to the following application components:

- files in the Kaspersky Industrial CyberSecurity for Nodes installation folder and other files of the application;
- registry keys with records belonging to the application;
- processes that the application runs.

> Self-defense mechanisms do not apply to Kaspersky Industrial CyberSecurity for Nodes processes initiated by untrusted parent processes.

The Self-Defense mechanisms of Kaspersky Industrial CyberSecurity for Nodes are enabled by default.

How to enable or disable Self-Defense in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Application settings** section.
4. In the **Security and reliability** block, click the **Settings** button.
5. This opens a window; in that window, select the **Security** tab.
6. In the **Self-Defense** block, use the **Protect application processes from external threats** check box to enable or disable Self-Defense.
7. Close the padlock to apply the policy to computers.
8. Click **OK** to save the changes.

How to enable or disable Self-Defense in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and in the results pane, follow the **Application properties** link.
2. This opens a window; in that window, select the **Security settings** tab.
3. In the **Self-Defense** block, use the **Protect application processes from external threats** check box to enable or disable Self-Defense.
4. Click **OK** to save the changes.

How to enable or disable Self-Defense in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Application Settings** section.
5. In the **Security and reliability** block, click the **Configure** button.

   The **Security and reliability** window opens.
6. In the **Self-Defense** block, use the **Protect application processes from external threats** check box to enable or disable Self-Defense.
7. Close the padlock to apply the policy to computers.
8. Click **OK** to save the changes.

Supporting AM-PPL technology

Kaspersky Industrial CyberSecurity for Nodes supports Antimalware Protected Process Light technology (hereinafter referred to as AM-PPL) from Microsoft. AM-PPL protects Kaspersky Industrial CyberSecurity for Nodes processes against malicious actions (for example, terminating the application). AM-PPL allows only trusted processes to run. Kaspersky Industrial CyberSecurity for Nodes processes are signed in accordance with Windows security requirements, and therefore they are trusted. For more details about AM-PPL technology, please visit the Microsoft website. AM-PPL technology is enabled by default.

Kaspersky Industrial CyberSecurity for Nodes also has built-in mechanisms for protecting application processes. AM-PPL support lets you delegate process security functions to the operating system. You can thereby increase the speed of the application and reduce the consumption of computer resources.

The application registers the Kaspersky Industrial CyberSecurity for Nodes (AVP) service and the Kaspersky Seamless Update Service (AVPSUS) service. The AM-PPL technology protects only the AVP service.

Keep the AM-PPL technology always active. AM-PPL is an important component of operating system protection. It is permissible to disable AM-PPL only in a separate testing environment for the purpose of troubleshooting the application.

AM-PPL technology is available for Windows 10 version 1703 (RS2) or later, and Windows Server 2019 operating systems.

To enable or disable AM-PPL technology:

1. Turn off the application's Self-Defense mechanism.

   The Self-Defense mechanism prevents modification and deletion of application processes in the computer memory, including changing the AM-PPL status.

2. Run the command line interpreter (cmd) as an administrator.

3. Go to the folder where the Kaspersky Industrial CyberSecurity for Nodes executable file is located.

4. To enable support for AM-PPL technology, run the following command:

   ```
   klpsm.exe enable
   ```

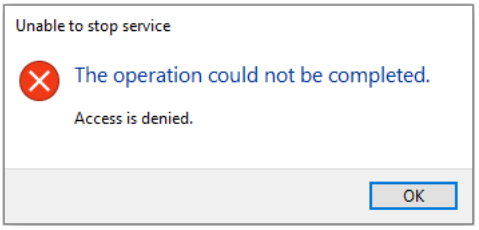
5. To disable support for AM-PPL technology, run the following command:

   ```
   klpsm.exe disable
   ```

6. Restart Kaspersky Industrial CyberSecurity for Nodes.

7. Resume the application's Self-Defense mechanism.

As a result, when a user attempts to stop the AVP service, a system window with an error message appears. The user can only manage application services from the Kaspersky Industrial CyberSecurity for Nodes interface.



Application services access error

Protecting operating system services

You can use the Protect operating system services functionality to allow or prohibit third-party applications from acting upon operating system services.

How to enable or disable operating system services protection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Application settings** section.
4. In the **Security and reliability** block, click the **Settings** button.
5. This opens a window; in that window, select the **Security** tab.
6. Use the **Protect operating system services** check box to enable or disable protection of the operating system services.

   If the protection of operating system services is enabled, third-party applications cannot act upon the processes of the operating system.

   If the protection of operating system services is disabled, third-party applications can act upon the processes of the operating system.

   After enabling or disabling the function, you must restart your computer to apply the changes.
7. Close the padlock to apply the policy to computers.
8. Click **OK** to save the changes.

How to enable or disable operating system services protection in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and in the results pane, follow the **Application properties** link.
2. This opens a window; in that window, select the **Security settings** tab.
3. Use the **Protect operating system services** check box to enable or disable protection of the operating system services.

   If the protection of operating system services is enabled, third-party applications cannot act upon the processes of the operating system.

   If the protection of operating system services is disabled, third-party applications can act upon the processes of the operating system.

   After enabling or disabling the function, you must restart your computer to apply the changes.
4. Click **OK** to save the changes.

How to enable or disable operating system services protection in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Application Settings** section.

5. In the **Security and reliability** block, click the **Configure** button.

   The **Security and reliability** window opens.

6. Use the **Protect operating system services** check box to enable or disable protection of the operating system services.

   If the protection of operating system services is enabled, third-party applications cannot act upon the processes of the operating system.

   If the protection of operating system services is disabled, third-party applications can act upon the processes of the operating system.

   After enabling or disabling the function, you must restart your computer to apply the changes.

7. Close the padlock to apply the policy to computers.

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

Configuring user permissions to manage Kaspersky Industrial CyberSecurity for Nodes

By default, all features of Kaspersky Industrial CyberSecurity for Nodes are accessible to the members of the Administrators group on the protected device, members of the KICS Administrators group created on the protected device when installing Kaspersky Industrial CyberSecurity for Nodes, and the SYSTEM group.

Users who are not registered in the list of Kaspersky Industrial CyberSecurity for Nodes users cannot open the Application Console.

You can allow or block access to specific functions of Kaspersky Industrial CyberSecurity for Nodes for individual users or groups of users.

About access permissions for Kaspersky Industrial CyberSecurity for Nodes functions

User rights	Description
Manage tasks	Ability to start / stop / pause / resume Kaspersky Industrial CyberSecurity for Nodes tasks.
Create and delete tasks	Ability to create and delete On-Demand Scan tasks.
Edit settings	Ability to: • Import Kaspersky Industrial CyberSecurity for Nodes settings from a configuration file. • Edit the application settings.
Read settings	Ability to: • View Kaspersky Industrial CyberSecurity for Nodes general settings and task settings. • Export Kaspersky Industrial CyberSecurity for Nodes settings to a configuration file. • View settings for task logs, system audit log, and notifications.
Manage storages	Ability to: • Move objects to Quarantine. • Remove objects from Quarantine and Backup. • Restore objects from Quarantine and Backup.
Manage logs	Ability to delete task logs and clear the system audit log.
Read logs	Ability to view Anti-Virus events in task logs and the system audit log.
Retrieve statistics	Ability to view statistics for each Kaspersky Industrial CyberSecurity for Nodes task.
Manage application licensing	Ability to activate Kaspersky Industrial CyberSecurity for Nodes.
Uninstall the application	Ability to uninstall Kaspersky Industrial CyberSecurity for Nodes.

User rights	Description
Read permissions	Ability to view the list of Kaspersky Industrial CyberSecurity for Nodes users and user access privileges.
Edit permissions	Ability to: • Edit the list of users with access to application management. • Edit user access permissions for Kaspersky Industrial CyberSecurity for Nodes functions.
Remote connection to application	Ability to remotely connect to the application using the Application Console. For remote access, the user must also have the access rights to the **Read settings** functionality.
Exit the application	Ability to exit the application using the Application Console.
Disable Kaspersky Security Center policy	Ability to disable the Kaspersky Security Center policy.
Export settings	Ability to export Kaspersky Industrial CyberSecurity for Nodes settings.
Edit Malfunction diagnosis	Ability to configure application tracing and memory dump recording settings.

How to configure user permissions to manage Kaspersky Industrial CyberSecurity for Nodes in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Supplementary**.
4. In the **User access permissions for application management** section, click **Settings**.
5. This opens a window; in that window, select the **Allow confirmation of actions with the application using credentials from manually created users** check box and set a password for the KLAdmin user account. The user account is automatically added to the list of user accounts.
6. If necessary, add user accounts to which you want to grant access to application management. To do so, click **Add** in the table of user accounts.

   This opens the form for configuring user access permissions.
7. Select the method that you want to use to add users:

   - **Select a user / group from Active Directory**. You can grant Kaspersky Industrial CyberSecurity for Nodes access to individual users or groups within the Active Directory domain. For example, if exiting the application is blocked for the Everyone group, you can grant the **Exit the application** permission to an individual user.
   - **Add a user / group of users manually**. You can create a user account that is not present in Active Directory and assign individual permissions to that user account. That is, you can create a *service user account* and use it instead of KLAdmin. This way, you do not need to share your KLAdmin password with other users or create new Active Directory user accounts. You can specify any user name and password. For example, you can grant the **Read logs** permission to the service user account. As a result, if viewing reports is prohibited to the 'All' group, you can open the reports using the service user account or the KLAdmin user account.

     To add a user or group of users manually, you must enable Password protection.
8. Select a user or group of users to which you want to grant access to managing the application.

9. In the **Permissions** list, configure user access permissions to application functionality.

10. Save your changes. To apply the policy on computers, close the padlocks .

How to configure user permissions to manage Kaspersky Industrial CyberSecurity for Nodes in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **User access permissions for application management** from the context menu of the node.

2. This opens a window; in that window, select the **Allow confirmation of actions with the application using credentials from manually created users** check box and set a password for the KLAdmin user account. The user account is automatically added to the list of user accounts.

3. If necessary, add user accounts to which you want to grant access to application management. To do so, click **Add** in the table of user accounts.

   This opens the form for configuring user access permissions.

4. Select the method that you want to use to add users:

   - **Select a user / group from Active Directory**. You can grant Kaspersky Industrial CyberSecurity for Nodes access to individual users or groups within the Active Directory domain. For example, if exiting the application is blocked for the Everyone group, you can grant the **Exit the application** permission to an individual user.

   - **Add a user / group of users manually**. You can create a user account that is not present in Active Directory and assign individual permissions to that user account. That is, you can create a *service user account* and use it instead of KLAdmin. This way, you do not need to share your KLAdmin password with other users or create new Active Directory user accounts. You can specify any user name and password. For example, you can grant the **Read logs** permission to the service user account. As a result, if viewing reports is prohibited to the 'All' group, you can open the reports using the service user account or the KLAdmin user account.

     To add a user or group of users manually, you must enable Password protection.

5. Select a user or group of users to which you want to grant access to managing the application.

6. In the **Permissions** list, configure user access permissions to application functionality.

7. Save your changes.

How to configure user access rights to manage Kaspersky Industrial CyberSecurity for Nodes in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Supplementary → User access permissions for application management** and click the **Configure** button.

5. This opens a window; in that window, select the **Allow confirmation of actions with the application using credentials from manually created users** check box and set a password for the KLAdmin user account. The user account is automatically added to the list of user accounts.

6. If necessary, add user accounts to which you want to grant access to application management. To do so, click **Add** in the table of user accounts.

   This opens the form for configuring user access permissions.

7. Select the method that you want to use to add users:

   - **Select a user / group from Active Directory**. You can grant Kaspersky Industrial CyberSecurity for Nodes access to individual users or groups within the Active Directory domain. For example, if exiting the application is blocked for the Everyone group, you can grant the **Exit the application** permission to an individual user.

   - **Add a user / group of users manually**. You can create a user account that is not present in Active Directory and assign individual permissions to that user account. That is, you can create a *service user account* and use it instead of KLAdmin. This way, you do not need to share your KLAdmin password with other users or create new Active Directory user accounts. You can specify any user name and password. For example, you can grant the **Read logs** permission to the service user account. As a result, if viewing reports is prohibited to the 'All' group, you can open the reports using the service user account or the KLAdmin user account.

     To add a user or group of users manually, you must enable Password protection.

8. Select a user or group of users to which you want to grant access to managing the application.

9. In the **Permissions** list, configure user access permissions to application functionality.

10. Save your changes. To apply the policy on computers, close the padlocks.

Configuring user access permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service

During installation, Kaspersky Industrial CyberSecurity for Nodes registers the application service, *Kaspersky Industrial CyberSecurity for Nodes Service*, in Windows. Thus, the application includes functional components that start at operating system startup. To reduce the risk of third-party access to application functionality and security settings of the protected device using the application service, you can restrict the permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service.

By default, the right to manage the Kaspersky Industrial CyberSecurity for Nodes Service is granted to users in the Administrators group on the protected device. Read permissions are granted to the SERVICE and INTERACTIVE groups, and read and execute permissions are granted to the SYSTEM group.

You cannot delete the SYSTEM user account or edit permissions for this account. If the permissions for the SYSTEM account are edited, the maximum privileges are restored for this account when you save the changes.

Users that have access to functionality at the 'Edit permissions' level can grant access permissions for managing the Kaspersky Industrial CyberSecurity for Nodes Service to other users registered on the protected device or included in the domain.

You can select one of the following preset levels of Kaspersky Industrial CyberSecurity for Nodes Service management access for a Kaspersky Industrial CyberSecurity for Nodes user or group:

- **Full control**: ability to view and edit general settings and user permissions for the Kaspersky Industrial CyberSecurity for Nodes Service, and ability to start and stop the Kaspersky Industrial CyberSecurity for Nodes Service.
- **Read**: ability to view general settings and user permissions of the Kaspersky Industrial CyberSecurity for Nodes Service.
- **Edit**: ability to view and edit general settings and user permissions of the Kaspersky Industrial CyberSecurity for Nodes Service.
- **Execute**: ability to start and stop the Kaspersky Industrial CyberSecurity for Nodes Service.

You can also configure advanced access permissions: allow or deny access to specific Kaspersky Industrial CyberSecurity for Nodes functions (see the table below).

Access permissions for the Kaspersky Industrial CyberSecurity for Nodes Service functionality

Feature	Description
Read service settings	Ability to view general settings and user permissions of the Kaspersky Industrial CyberSecurity for Nodes Service.
Request service status from Service Control Manager	Ability to request the execution status of the Kaspersky Industrial CyberSecurity for Nodes Service from the Microsoft Windows Service Control Manager.
Request service status	Ability to request the service execution status from the Kaspersky Industrial CyberSecurity for Nodes Service.
Read list of dependent services	Ability to view the list of services which the Kaspersky Industrial CyberSecurity for Nodes Service depends on and which depend on the Kaspersky Industrial CyberSecurity for Nodes Service.
Modify service settings	Ability to view and edit general settings and user permissions of the Kaspersky Industrial CyberSecurity for Nodes Service.
Start service	Ability to start the Kaspersky Industrial CyberSecurity for Nodes Service.
Stop service	Ability to stop the Kaspersky Industrial CyberSecurity for Nodes Service.
Pause / resume service	Ability to pause and resume the Kaspersky Industrial CyberSecurity for Nodes Service.
Read permissions	Ability to view the list of the Kaspersky Industrial CyberSecurity for Nodes Service users and each user's access privileges.
Edit permissions	Ability to: • Add or remove the Kaspersky Industrial CyberSecurity for Nodes Service users. • Edit user access permissions for the Kaspersky Industrial CyberSecurity for Nodes Service.
Remove service	Ability to deregister the Kaspersky Industrial CyberSecurity for Nodes Service in the Microsoft Windows Service Control Manager.
User defined requests to service	Ability to create and send user requests to the Kaspersky Industrial CyberSecurity for Nodes Service.

You can edit the list of users and user groups allowed to manage the Kaspersky Industrial CyberSecurity for Nodes Service, and also edit the access permissions of those users and user groups.

How to configure user permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Supplementary**.

4. In the **User access permissions for KICS for Nodes Service management** section, click **Settings**.

   This opens the form for configuring user access permissions.

5. Add an Active Directory user or group for which you want to configure the Kaspersky Industrial CyberSecurity for Nodes Service user permissions.

6. Select a user or group of users to which you want to grant access to managing the application.

7. In the list of permissions, configure user permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service.

8. If necessary, configure special permissions for users:

   a. Click **Additional**.

   b. This opens a window; in that window, select a user account.

   c. Double-click to open the user account properties.

   d. This opens a window; in that window, click the **Show additional permissions** link.

   e. This opens a window; in that window, configure special permissions for the user.

9. Save your changes. To apply the policy on computers, close the padlocks .

How to configure user permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **User access permissions for KICS for Nodes Service management** from the context menu of the node.

2. In the window that opens, in the **Permissions** block, click the **Add** button.

   This opens the form for configuring user access permissions.

3. Add an Active Directory user or group for which you want to configure the Kaspersky Industrial CyberSecurity for Nodes Service user permissions.

4. Select a user or group of users to which you want to grant access to managing the application.

5. In the list of permissions, configure user permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service.

6. If necessary, configure special permissions for users:

   a. Click **Additional**.

   b. This opens a window; in that window, select a user account.

   c. Double-click to open the user account properties.

   d. This opens a window; in that window, click the **Show additional permissions** link.

   e. This opens a window; in that window, configure special permissions for the user.

7. Save your changes.

How to configure user permissions to manage the Kaspersky Industrial CyberSecurity for Nodes Service in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Supplementary** → **User access permissions for KICS for Nodes Service management** and click the **Configure** button.

   The **User access permissions for KICS for Nodes Service management** window opens.
5. Add an Active Directory user or group for which you want to configure the Kaspersky Industrial CyberSecurity for Nodes Service user permissions.
6. Select a user or group of users to which you want to grant access to managing the application.

   > You cannot configure special permissions to manage the application service in the Web Console.
7. Save your changes. To apply the policy on computers, close the padlocks.

Password-protected access to Kaspersky Industrial CyberSecurity for Nodes functionality

Configuring user rights lets you restrict access to application management and registered services by configuring user permissions. You can also set password protection in the Kaspersky Industrial CyberSecurity for Nodes settings for additional protection of critical operations.

When a user attempts to perform a password-protected action, Kaspersky Industrial CyberSecurity for Nodes prompts the user for the user name and password or to use a token for authentication.

User name and password

Password protection supports the following accounts:

- **KLAdmin**. An Administrator account with unrestricted access to Kaspersky Industrial CyberSecurity for Nodes. The KLAdmin account has the right to perform any action that is password-protected. The permissions for the KLAdmin account cannot be revoked. When you enable password protection, Kaspersky Industrial CyberSecurity for Nodes prompts you to set a password for the KLAdmin account.
- **Account added manually**. An account outside the Active Directory domain. You can use this service account instead of KLAdmin if you do not want to share the administrator password. You can set any user name and password and configure individual permissions.

- **The Everyone group**. A built-in Windows group that includes all users within the corporate network. Users in the Everyone group can access the application according to the permissions that are granted to them.

- **Individual users or groups**. User accounts for which you can configure individual permissions. For example, if an action is blocked for the Everyone group, you can allow this action for an individual user or a group.

The Kaspersky Industrial CyberSecurity for Nodes interface disguises the specified password on screen. Kaspersky Industrial CyberSecurity for Nodes stores the password as a checksum calculated when the password is entered.

Kaspersky Industrial CyberSecurity for Nodes doesn't check password strength and doesn't block password entry after a number of failed attempts.

When creating a password, you are recommended to meet the following conditions:

- The password doesn't contain the account name or computer name.
- The password is at least 8 characters long.
- The password contains characters that match at least three of the following categories:
  - Uppercase Latin letters (A-Z)
  - Lowercase Latin letters (a-z)
  - Numerals (0-9)
  - Exclamation mark (!), dollar sign ($), pound sign (#) and percent sign (%)

Token

To access the Kaspersky Industrial CyberSecurity for Nodes functionality, you must select the appropriate user certificate from the list of certificates stored on the connected token and enter your PIN. Token-based authentication is available only to users within the Active Directory domain. The administrator can configure permissions for an individual user or a group. For token-based authentication to work, you must deploy a trusted PKI infrastructure and install special software to manage the token.

How to password-protect access to Kaspersky Industrial CyberSecurity for Nodes functionality in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Supplementary**.
4. In the **User access permissions for application management** section, click **Settings**.
5. In the window that opens, select the **Allow confirmation of actions with the application using credentials from manually created users** check box.
6. If necessary, clear the **Request password to confirm critical actions** check box.

If this functionality is enabled, the application requests a user name and password when deleting, modifying, or recovering the application, and when performing actions on the command line that may lower the protection level of the device.

If this functionality is disabled, and the current user has the necessary rights, Kaspersky Industrial CyberSecurity for Nodes does not request credentials. This option is enabled by default.

> If an empty Windows password is set for the current user, you need to enter the credentials of a user that possesses the necessary rights and has a non-empty password.

7. Specify the password for the KLAdmin user account.
8. If necessary, add user accounts to which you want to grant access to application management:
   a. Click **Add**.
      This opens the form for configuring user access permissions.
   b. In the window that opens, select the method for adding users: **Add a user / group of users manually**.
   c. Specify a user name and password.
   d. In the **Permissions** list, configure user access permissions to application functionality.
9. Save your changes. To apply the policy on computers, close the padlocks.

How to password-protect access to Kaspersky Industrial CyberSecurity for Nodes functionality in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **User access permissions for application management** from the context menu of the node.
2. In the window that opens, select the **Allow confirmation of actions with the application using credentials from manually created users** check box.
3. If necessary, clear the **Request password to confirm critical actions** check box.
   If this functionality is enabled, the application requests a user name and password when deleting, modifying, or recovering the application, and when performing actions on the command line that may lower the protection level of the device.
   If this functionality is disabled, and the current user has the necessary rights, Kaspersky Industrial CyberSecurity for Nodes does not request credentials. This option is enabled by default.

   > If an empty Windows password is set for the current user, you need to enter the credentials of a user that possesses the necessary rights and has a non-empty password.

4. Specify the password for the KLAdmin user account.
5. If necessary, add user accounts to which you want to grant access to application management:
   a. Click **Add**.
      This opens the form for configuring user access permissions.
   b. In the window that opens, select the method for adding users: **Add a user / group of users manually**.

c. Specify a user name and password.

d. In the **Permissions** list, configure user access permissions to application functionality.

6. Save your changes.

How to password-protect access to Kaspersky Industrial CyberSecurity for Nodes functionality in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Supplementary** → **User access permissions for application management** and click the **Configure** button.
5. In the window that opens, select the **Allow confirmation of actions with the application using credentials from manually created users** check box.
6. If necessary, clear the **Request password to confirm critical actions** check box.

   If this functionality is enabled, the application requests a user name and password when deleting, modifying, or recovering the application, and when performing actions on the command line that may lower the protection level of the device.

   If this functionality is disabled, and the current user has the necessary rights, Kaspersky Industrial CyberSecurity for Nodes does not request credentials. This option is enabled by default.

   > If an empty Windows password is set for the current user, you need to enter the credentials of a user that possesses the necessary rights and has a non-empty password.

7. Specify the password for the KLAdmin user account.
8. If necessary, add user accounts to which you want to grant access to application management:

   a. Click **Add**.

   This opens the form for configuring user access permissions.

   b. In the window that opens, select the method for adding users: **Add a user / group of users manually**.

   c. Specify a user name and password.

   d. In the **Permissions** list, configure user access permissions to application functionality.
9. Save your changes. To apply the policy on computers, close the padlocks.

This password cannot be recovered. Losing your password results in complete loss of control over the application. Moreover, you will not be able to remove the application from the protected device.

You can reset the password at any time. To do that, clear the **Allow confirmation of actions with the application using credentials from manually created users** check box and save changes. Password protection will be disabled and the old password checksum will be removed. Repeat the password creation process with a new password.

Secure Desktop notifications

Kaspersky Industrial CyberSecurity for Nodes supports the (Secure Desktop) functionality. The purpose of this functionality is to confirm actions that can potentially lower the security level of the computer. This functionality lets an application display a confirmation dialog that is isolated from other processes. This functionality uses elevated rights to secure the request. In this way, only the user can confirm the action and not the malware.

Kaspersky Industrial CyberSecurity for Nodes displays Secure Desktop notifications to confirm the following actions:

- Tracing enabled or disabled
- Application settings exported or imported
- Protection paused
- Application exited
- Active key deleted
- Kaspersky Industrial CyberSecurity for Nodes uninstalled
- Device Control disabled
- Real-Time File Protection disabled
- Kaspersky Security Center policy disabled
- Reports viewed
- Files restored from Backup
- Kaspersky Industrial CyberSecurity for Nodes settings modified
- Application tasks managed in ways other than starting

How to enable or disable Secure Desktop notifications in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Application settings** section.
4. In the **Security and reliability** block, click the **Settings** button.
5. This opens a window; in that window, select the **Security** tab.

6. In the **Self-Defense** block, select or clear the **Enable Secure Desktop notifications** check box to enable or disable Secure Desktop notifications.

   If Self-Defense mechanisms are disabled, the **Enable Secure Desktop notifications** check box is not available.

7. Close the padlock to apply the policy to computers.

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

How to enable or disable Secure Desktop notifications in the Administration Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and in the results pane, follow the **Application properties** link.

2. This opens a window; in that window, select the **Security settings** tab.

3. In the **Self-Defense** block, select or clear the **Enable Secure Desktop notifications** check box to enable or disable Secure Desktop notifications.

   If Self-Defense mechanisms are disabled, the **Enable Secure Desktop notifications** check box is not available.

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

How to enable or disable Secure Desktop notifications in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Application Settings** section.

5. In the **Security and reliability** block, click the **Configure** button.

   The **Security and reliability** window opens.

6. In the **Self-Defense** block, select or clear the **Enable Secure Desktop notifications** check box to enable or disable Secure Desktop notifications.

   If Self-Defense mechanisms are disabled, the **Enable Secure Desktop notifications** check box is not available.

7. Close the padlock to apply the policy to computers.

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

Trusted zone

A *trusted zone* is a system administrator-configured list of objects and applications that Kaspersky Industrial CyberSecurity for Nodes does not monitor when active.

The administrator forms the trusted zone independently, taking into account the features of the objects that are handled and the applications that are installed on the computer. It may be necessary to include objects and applications in the trusted zone when Kaspersky Industrial CyberSecurity for Nodes blocks access to a certain object or application, if you are sure that the object or application is harmless. An administrator can also allow a user to create their own local trusted zone for a specific computer. This way, users can create their own local lists of exclusions and trusted applications in addition to the general trusted zone in a policy.

You can also add EDR telemetry to the trusted zone. This allows to optimize data that the application sends to the Telemetry server for the Kaspersky Anti Targeted Attack Platform (EDR) solution.

Predefined scan exclusions and trusted applications have been added to the trusted zone. Predefined scan exclusions and trusted applications help quickly configure Kaspersky Industrial CyberSecurity for Nodes without manually creating a trusted zone.

Creating a scan exclusion

A *scan exclusion* is a set of conditions that must be fulfilled so that Kaspersky Industrial CyberSecurity for Nodes will not scan a particular object for viruses and other threats.

Scan exclusions can be used by the following application components and tasks:

- **Real-Time File Protection**
- **On-Demand Scan**
- **Anti-Cryptor**
- **AMSI Scanner**
- **Network Threat Protection**

Kaspersky Industrial CyberSecurity for Nodes does not scan an object if the drive or folder containing this object is included in the scan scope at the start of one of the scan tasks. However, the scan exclusion is not applied when a custom scan task is started for this particular object.

Kaspersky Industrial CyberSecurity for Nodes does not support exclusion lists containing over 5000 objects.

How to create a scan exclusion in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.

3. In the policy window, select **Supplementary** → **Trusted zone** and click **Settings**.

4. Select the **Scan exclusions** tab.

5. Select the **Merge values when inheriting** check box if you want to create a consolidated list of exclusions for all computers in the company. The lists of exclusions in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Exclusions from the parent policy are displayed in child policies in a read-only view. Changing or deleting exclusions of the parent policy is not possible.

6. Select the **Allow use of local exclusions** check box if you want to enable the user to create a local list of exclusions. This way, a user can create their own local list of exclusions in addition to the general list of exclusions generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.

   If the check box is cleared, the user can access only the general list of exclusions generated in the policy. Also, if this check box is cleared, Kaspersky Industrial CyberSecurity for Nodes hides the consolidated list of scan exclusions in the Application Console.

7. Click **Add** and select an action:

   - **Category**. You can group scan exclusions into separate categories. To create a new category, enter the name of the category and add at least one scan exclusion to the category.

   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new scan exclusion to the root of the list.

   - **New exclusion to selected category**. To add a new scan exclusion to a specific category, select a category.

   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add exclusions from the list of predefined scan exclusions.

8. To exclude a file or folder from scan, select the **File or folder** check box. Click the **select file or folder** link to open a window, and in that window, select a file or folder by clicking **Browse**.

   You can also enter the path manually. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

   - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

   - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.

   - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

     You can use masks at the beginning, in the middle or at the end of the file path. For example, if you want to add a folder for all users to exclusions, enter the `?:\Users\*\Folder\` mask.

9. To exclude a predefined area from scan, select the **Predefined scope** check box. Click the **select predefined scope** link to open a window, and in that window, select one the standard scopes on the protected device.

10. To exclude the specific objects from scan, select the **Type of detected object** check box. Click the **enter object names** link, click the **Add** button, and in the displayed window, enter the name of the object type according to the Kaspersky Encyclopedia classification (for example, `Email-Worm`, `Rootkit`, or `RemoteAdmin`).

    You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, Kaspersky Industrial CyberSecurity for Nodes excludes `Client-IRC`, `Client-P2P` and `Client-SMTP` objects from scans.

11. To exclude an individual file from scan, select the **Object hash** check box. Click the **enter object hash** link to open a window, and in that window, enter a file hash.

    If the file is modified, the file hash will also be modified. If this happens, the modified file will not be added to exclusions.

12. In the **Rule usage scope** block, select the components that you want the scan exclusion to apply to.

13. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

14. Save changes to add the exclusion to the list. You can disable the exclusion at any time using the check box next to the object.

How to create a scan exclusion in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

    The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Supplementary** → **Trusted zone** and click the **Configure** button.

5. Select the **Scan exclusions** tab.

6. Select the **Merge values when inheriting** check box if you want to create a consolidated list of exclusions for all computers in the company. The lists of exclusions in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Exclusions from the parent policy are displayed in child policies in a read-only view. Changing or deleting exclusions of the parent policy is not possible.

7. Select the **Allow use of local exclusions** check box if you want to enable the user to create a local list of exclusions. This way, a user can create their own local list of exclusions in addition to the general list of exclusions generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.

    If the check box is cleared, the user can access only the general list of exclusions generated in the policy. Also, if this check box is cleared, Kaspersky Industrial CyberSecurity for Nodes hides the consolidated list of scan exclusions in the Application Console.

8. Click **Add** and select an action:

   - **Category**. You can group scan exclusions into separate categories. To create a new category, enter the name of the category and add at least one scan exclusion to the category.
   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new scan exclusion to the root of the list.
   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add exclusions from the list of predefined scan exclusions.

9. If you want to exclude a file or folder from scanning, select **File or folder** and select the check box in the field with the same name. Specify the path to the file or folder.

   Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

   - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
   - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.
   - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

     You can use masks at the beginning, in the middle or at the end of the file path. For example, if you want to add a folder for all users to exclusions, enter the `?:\Users\*\Folder\` mask.

10. To exclude a predefined scope from scanning, select **Predefined scope**. In the drop-down list, select one of the standard scopes on the protected device.

11. If you want to exclude certain objects from scanning, select the **Type of detected object** check box and enter the name of the object type according to the Kaspersky Encyclopedia classification (for example, `Email-Worm`, `Rootkit`, or `RemoteAdmin`).

    You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, Kaspersky Industrial CyberSecurity for Nodes excludes *Client-IRC*, *Client-P2P* and *Client-SMTP* objects from scans.

12. To exclude an individual file from scanning, select the **Object hash** check box and add a hash from a file or a list of events.

    If the file is modified, the file hash will also be modified. If this happens, the modified file will not be added to exclusions.

13. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

14. In the **Protection components** block, select the components that you want the scan exclusion to apply to.

15. The new exclusion will be added to the list. You can disable the exclusion at any time using the check box in the **Status** column.

16. Save your changes.

How to create a scan exclusion in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

   The **Configure Trusted zone settings** window opens.

2. In the **Exclusions** section, click the **Settings** button next to the **Scan exclusions** block.

3. Click **Add** and select an action:

   - **Category**. You can group scan exclusions into separate categories. To create a new category, enter the name of the category and add at least one scan exclusion to the category.
   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new scan exclusion to the root of the list.
   - **New exclusion to selected category**. To add a new scan exclusion to a specific category, select a category.
   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add exclusions from the list of predefined scan exclusions.

4. To exclude a file or folder from scan, select the **File or folder** check box. Click the **Select file or folder** link to open a window, and in that window, select a file or folder by clicking **Browse**.

   You can also enter the path manually. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

   - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
   - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.
   - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

     You can use masks at the beginning, in the middle or at the end of the file path. For example, if you want to add a folder for all users to exclusions, enter the `?:\Users\*\Folder\` mask.

5. To exclude a predefined area from scan, select the **Predefined scope** check box. Click the **select predefined scope** link to open a window, and in that window, select one the standard scopes on the protected device.

6. To exclude the specific objects from scan, select the **Type of detected object** check box. Click the **enter object names** link, click the **Add** button, and in the displayed window, enter the name of the object type according to the Kaspersky Encyclopedia classification (for example, `Email-Worm`, `Rootkit`, or `RemoteAdmin`).

   You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, Kaspersky Industrial CyberSecurity for Nodes excludes `Client-IRC`, `Client-P2P` and `Client-SMTP` objects from scans.

7. To exclude an individual file from scan, select the **Object hash** check box. Click the **enter object hash** link to open a window, and in that window, enter a file hash.

   If the file is modified, the file hash will also be modified. If this happens, the modified file will not be added to exclusions.

8. In the **Rule usage scope** block, select the components that you want the scan exclusion to apply to.

9. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

10. Save changes to add the exclusion to the list. You can disable the exclusion at any time using the check box next to the object.

Path mask examples:
Paths to files located in any folder:

- The mask `*.exe` will include all paths to files that have the exe extension.
- The mask `example*` will include all paths to files named EXAMPLE.

Paths to files located in a specified folder:

- The `C:\dir\*.*` mask will include all paths to files located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
- The mask `C:\dir\*` will include all paths to files located in the C:\dir\ folder, including subfolders.
- The mask `C:\dir\` will include all paths to files located in the C:\dir\ folder, including subfolders.
- The mask `C:\dir\*.exe` will include all paths to files with the .EXE extension located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
- The mask `C:\dir\test` will include all paths to files named "test" located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
- The mask `C:\dir\*\test` will include all paths to files named "test" located in the C:\dir\ folder and in the subfolders of C:\dir\.
- The mask `C:\dir1\*\dir3\` will include all paths to files in dir3 subfolders one level into the C:\dir1\ folder.
- The mask `C:\dir1\**\dirN\` will include all paths to files in dirN subfolders in the C:\dir1\ folder at any level.

Paths to files located in all folders with a specified name:

- The mask `dir\*.*` will include all paths to files in folders named "dir", but not in the subfolders of those folders.
- The mask `dir\*` will include all paths to files in folders named "dir", but not in the subfolders of those folders.
- The mask `dir\` will include all paths to files in folders named "dir", but not in the subfolders of those folders.
- The mask `dir\*.exe` will include all paths to files with the .EXE extension in folders named "dir", but not in the subfolders of those folders.
- The mask `dir\test` will include all paths to files named "test" in folders named "dir", but not in the subfolders of those folders.

Selecting types of detectable objects

To select types of detectable objects:

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and do one of the following:

   - Click the **Configure Trusted zone settings** link in the results pane of the node.
   - Select **Trusted zone** in the node's context menu.

   The **Configure Trusted zone settings** window opens.

2. In the **Types of detected objects** section, click **Settings**.

3. In the window that opens, select check boxes opposite the types of objects that you want Kaspersky Industrial CyberSecurity for Nodes to detect:

   - **Viruses and worms**

     Subcategory: viruses and worms (Viruses_and_Worms)

     Danger level: High

     Classic viruses and worms perform actions that are not authorized by the user. They can create copies of themselves which are able to self-replicate.

     Classic virus

     When a classic virus infiltrates a computer, it infects a file, activates, performs malicious actions, and adds copies of itself to other files.

     A classic virus multiplies only on local resources of the computer; it cannot penetrate other computers on its own. It can be passed to another computer only if it adds a copy of itself to a file that is stored in a shared folder or on an inserted CD, or if the user forwards an email message with an attached infected file.

     Classic virus code can penetrate various areas of computers, operating systems, and applications. Depending on the environment, viruses are divided into *file viruses*, *boot viruses*, *script viruses*, and *macro viruses*.

     Viruses can infect files by using a variety of techniques. *Overwriting* viruses write their code over the code of the file that is infected, thus erasing the file's content. The infected file stops functioning and cannot be restored. *Parasitic* viruses modify files, leaving them fully or partially functional. *Companion viruses* do not modify files, but instead create duplicates. When an infected file is opened, a duplicate of it (what is actually a virus) is started. The following types of viruses are also encountered: *link viruses*, *OBJ viruses*, *LIB viruses*, *source code* viruses, and many others.

     Worm

     As with a classic virus, the code of a worm is activated and performs malicious actions after it infiltrates a computer. Worms are so named because of their ability to "crawl" from one computer to another and to spread copies via numerous data channels without the user's permission.

The main feature that allows differentiating between various types of worms is the way they spread. The following table provides an overview of various types of worms, which are classified by the way in which they spread.

Ways in which worms spread

Type	Name	Description
Email-Worm	Email-Worm	They spread via email. An infected email message contains an attached file with a copy of a worm, or a link to a file that is uploaded to a website which may have been hacked or created exclusively for that purpose. When you open the attached file, the worm is activated. When you click the link, download, and then open the file, the worm also starts performing its malicious actions. After that, it goes on spreading copies of itself, searching for other email addresses and sending infected messages to them.
IM-Worm	IM client worms	They spread through IM clients. Usually, such worms send messages that contain a link to a file with a copy of the worm on a website, making use of the user's contact lists. When the user downloads and opens the file, the worm activates.
IRC-Worm	Internet chat worms	They spread via Internet Relay Chats, service systems which allow communicating with other people over the Internet in real time. These worms publish a file with a copy of themselves or a link to the file in an Internet chat. When the user downloads and opens the file, the worm activates.
Net-Worm	Network worms	These worms spread over computer networks. Unlike other types of worms, a typical network worm spreads without the user's participation. It scans the local network for computers that contain programs with vulnerabilities. To do this, it sends a specially formed network packet (exploit) which contains the worm code or a part of it. If a "vulnerable" computer is on the network, it receives such a network packet. When the worm completely penetrates the computer, it activates.
P2P-Worm	File sharing network worms	They spread over peer-to-peer file sharing networks. To infiltrate a P2P network, the worm copies itself into a file sharing folder which is usually located on the user's computer. The P2P network displays information about this file so that the user may "find" the infected file on the network like any other file, and then download and open it. More sophisticated worms emulate the network protocol of a specific P2P network: they return positive responses to search queries and offer copies of themselves for download.
Worm	Other types of worms	Other types of worms include: • Worms that spread copies of themselves over network resources. By using the functions of the operating system, they scan available network folders, connect to computers on the Internet, and attempt to obtain full access to their disk drives. Unlike the previously described types of worms, other types of worms activate not on their own, but when the user opens a file that contains a copy of the worm. • Worms that do not use any of the methods described in the previous table to spread (for example, those that spread over cell phones).

- **Trojans**

  Subcategory: Trojans

  Danger level: High

  Unlike worms and viruses, Trojans do not self-replicate. For example, they penetrate a computer via email or a browser when the user visits an infected web page. Trojans are started with the user's participation. They begin performing their malicious actions right after they are started.

  Different Trojans behave differently on infected computers. The main functions of Trojans consist in blocking, modifying, or destroying information, and disabling computers or networks. Trojans can also receive or send files, run them, display messages on the screen, request web pages, download and install programs, and restart the computer.

  Hackers often use "sets" of various Trojans.

  Types of Trojan behavior are described in the following table.

Types of Trojan behavior on an infected computer

Type	Name	Description
Trojan-ArcBomb	Trojans – "archive bombs"	When unpacked, these archives grow in size to such an extent that the computer's operation is impacted. When the user attempts to unpack such an archive, the computer may slow down or freeze; the hard disk may become filled with "empty" data. "Archive bombs" are especially dangerous to file and mail servers. If the server uses an automatic system to process incoming information, an "archive bomb" may halt the server.
Backdoor	Trojans for remote administration	They are considered the most dangerous type of Trojan. In their functions, they are similar to remote administration applications that are installed on computers. These programs install themselves on the computer without being noticed by the user, allowing the intruder to manage the computer remotely.
Trojan	Trojans	They include the following malicious applications: • **Classic Trojans**. These programs perform only the main functions of Trojans: blocking, modifying or destroying information, and disabling computers or networks. They do not have any advanced features, unlike the other types of Trojans that are described in the table. • **Versatile Trojans**. These programs have advanced features typical of several types of Trojans.
Trojan-Ransom	Ransom Trojans	They take the user's information "hostage", modifying or blocking it, or impact the computer's operation so that the user loses the ability to use information. The intruder demands a ransom from the user, promising to send an application to restore the computer's performance and the data that had been stored on it.
Trojan-Clicker	Trojan clickers	They access web pages from the user's computer, either by sending commands to a browser on their own or by changing the web addresses that are specified in operating system files. By using these programs, intruders perpetrate network attacks and increase website visits, increasing the number of displays of banner ads.
Trojan-Downloader	Trojan downloaders	They access the intruder's web page, download other malicious applications from it, and install them on the user's computer. They can contain the file name of the malicious application to download, or receive it from the web page that is accessed.
Trojan-Dropper	Trojan droppers	They contain other Trojans which they install on the hard drive and then install. Intruders may use Trojan Dropper–type programs for the following goals: • Install a malicious application without being noticed by the user: Trojan Dropper–type programs display no messages, or display fake messages which inform, for example, of an error in an archive or an incompatible version of the operating system. • Protect another known malicious application from detection: not all anti-virus software can detect a malicious application within a Trojan Dropper–type application.
Trojan-Notifier	Trojan notifiers	They inform an intruder that the infected computer is accessible, sending the intruder information about the computer: IP address, number of opened port, or email address. They connect with the intruder via email, FTP, accessing the intruder's web page, or in another way. Trojan Notifier–type programs are often used in sets that are made of several Trojans. They notify the intruder that other Trojans have been successfully installed on the user's computer.
Trojan-Proxy	Trojan proxies	They allow the intruder to anonymously access web pages by using the user's computer; they are often used for sending spam.
Trojan-PSW	Password-stealing-ware	Password-stealing-ware is a kind of Trojan that steals user accounts, such as software registration data. These Trojans find confidential data in system files and in the registry and send it to the "attacker" by email, via FTP, by accessing the intruder's web page, or in another way. Some of these Trojans are categorized into separate types that are described in this table. These are Trojans that steal bank accounts (Trojan-Banker), steal data from users of IM clients (Trojan-IM), and steal information from users of online games (Trojan-GameThief).
Trojan-Spy	Trojan spies	They spy on the user, collecting information about the actions that the user makes while working at the computer. They may intercept the data that the user enters at the keyboard, take screenshots, or collect lists of active applications. After they receive the information, they transfer it to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Trojan-DDoS	Trojan network attackers	They send numerous requests from the user's computer to a remote server. The server lacks resources to process all requests, so it stops functioning (Denial of Service, or simply DoS). Hackers often infect many computers with these programs so that they can use the computers to attack a single server simultaneously. DoS programs perpetrate an attack from a single computer with the user's knowledge. DDoS (Distributed DoS) programs perpetrate distributed attacks from several computers without being noticed by the user of the infected computer.

Type	Name	Description
Trojan-IM	Trojans that steal information from users of IM clients	They steal account numbers and passwords of IM client users. They transfer the data to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Rootkit	Rootkits	They mask other malicious applications and their activity, thus prolonging the applications' persistence in the operating system. They can also conceal files, processes in an infected computer's memory, or registry keys which run malicious applications. The rootkits can mask data exchange between applications on the user's computer and other computers on the network.
Trojan-SMS	Trojans in the form of SMS messages	They infect cell phones, sending SMS messages to premium-rate phone numbers.
Trojan-GameThief	Trojans that steal information from users of online games	They steal account credentials from users of online games, after which they send the data to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Trojan-Banker	Trojans that steal bank accounts	They steal bank account data or e-money system data; send the data to the hacker by email, via FTP, by accessing the hacker's web page, or by using another method.
Trojan-Mailfinder	Trojans that collect email addresses	They collect email addresses that stored on a computer and send them to the intruder by email, via FTP, by accessing the intruder's web page, or in another way. Intruders may send spam to the addresses they have collected.

- **Malicious tools**

  Subcategory: Malicious tools

  Danger level: Medium

  Unlike other types of malware, malicious tools do not perform their actions right after they are started. They can be safely stored and started on the user's computer. Intruders often use the features of these programs to create viruses, worms, and Trojans, perpetrate network attacks on remote servers, hack computers, or perform other malicious actions.

  Various features of malicious tools are grouped by the types that are described in the following table.

  Features of malicious tools

Type	Name	Description
Constructor	Constructors	They allow creating new viruses, worms, and Trojans. Some constructors boast a standard window-based interface in which the user can select the type of malicious application to create, the way of counteracting debuggers, and other features.
Dos	Network attacks	They send numerous requests from the user's computer to a remote server. The server lacks resources to process all requests, so it stops functioning (Denial of Service, or simply DoS).
Exploit	Exploits	An *exploit* is a set of data or a program code that uses vulnerabilities of the application in which it is processed, performing a malicious action on a computer. For example, an exploit can write or read files, or request "infected" web pages. Different exploits use vulnerabilities in different applications or network services. Disguised as a network packet, an exploit is transmitted over the network to numerous computers, searching for computers with vulnerable network services. An exploit in a DOC file uses the vulnerabilities of a text editor. It may start performing the actions that are preprogrammed by the hacker when the user opens the infected file. An exploit that is embedded in an email message searches for vulnerabilities in any email client. It may start performing a malicious action as soon as the user opens the infected message in this email client. Net-Worms spread over networks by using exploits. Nuker exploits are network packets that disable computers.
FileCryptor	Encryptors	They encrypt other malicious applications to conceal them from the anti-virus application.
Flooder	Programs for "contaminating" networks	They send numerous messages over network channels. This type of tools includes, for example, programs that contaminate Internet Relay Chats. Flooder-type tools do not include programs that "contaminate" channels that are used by email, IM clients, and mobile communication systems. These programs are distinguished as separate types that are described in the table (Email-Flooder, IM-Flooder, and SMS-Flooder).

Type	Name	Description
HackTool	Hacking tools	They make it possible to hack the computer on which they are installed or attack another computer (for example, by adding new system accounts without the user's permission or by erasing system logs to conceal traces of their presence in the operating system). This type of tools includes some sniffers which feature malicious functions, such as password interception. Sniffers are programs that allow viewing network traffic.
Hoax	Hoaxes	They alarm the user with virus-like messages: they may "detect a virus" in an uninfected file or notify the user that the disk has been formatted, although this has not happened in reality.
Spoofer	Spoofing tools	They send messages and network requests with a fake address of the sender. Intruders use Spoofer-type tools to pass themselves off as the true senders of messages, for example.
VirTool	Tools that modify malicious applications	They allow modifying other malware programs, concealing them from anti-virus applications.
Email-Flooder	Programs that "contaminate" email addresses	They send numerous messages to various email addresses, thus "contaminating" them. A large volume of incoming messages prevents users from viewing useful messages in their inboxes.
IM-Flooder	Programs that "contaminate" traffic of IM clients	They flood users of IM clients with messages. A large volume of messages prevents users from viewing useful incoming messages.
SMS-Flooder	Programs that "contaminate" traffic with SMS messages	They send numerous SMS messages to cell phones.

- **Adware**

  Subcategory: Advertising software (Adware)

  Danger level: Medium

  Adware displays advertising information to the user. Adware programs display banner ads in the interfaces of other programs and redirect search queries to advertising web pages. Some of them collect marketing information about the user and send it to the developer: this information may include the names of the websites that are visited by the user or the content of the user's search queries. Unlike Trojan-Spy–type programs, adware sends this information to the developer with the user's permission.

- **Auto-dialers**

  Subcategory: Auto-dialers (Dialer).

  Danger level: Medium

  Auto-dialers can surreptitiously establish phone connections using a modem.

- **Legitimate software that can be used by intruders to damage your computer or personal data**

  Subcategory: Legitimate software that can be used by intruders to damage your computer or personal data.

  Danger level: Medium

  Most of these applications are useful, so many users run them. These applications include IRC clients, auto-dialers, file download programs, computer system activity monitors, password utilities, and internet servers for FTP, HTTP, and Telnet.

  However, if intruders gain access to these programs, or if they plant them on the user's computer, some of the application's features may be used to violate security.

These applications differ by function; their types are described in the following table.

Type	Name	Description
Client-IRC	Internet chat clients	Users install these programs to talk to people in Internet Relay Chats. Intruders use them to spread malware.
Downloader	Programs for downloading	They can download files from web pages in hidden mode.
Monitor	Programs for monitoring	They allow monitoring activity on the computer on which they are installed (seeing which applications are active and how they exchange data with applications that are installed on other computers).
PSWTool	Password restorers	They allow viewing and restoring forgotten passwords. Intruders secretly implant them on users' computers with the same purpose.
RemoteAdmin	Remote administration programs	They are widely used by system administrators. These programs allow obtaining access to the interface of a remote computer to monitor and manage it. Intruders secretly implant them on users' computers with the same purpose: to monitor and manage remote computers. Legal remote administration programs differ from backdoor-type Trojans for remote administration. Trojans have the ability to penetrate the operating system independently and install themselves; legal programs are unable to do so.
Server-FTP	FTP servers	They function as FTP servers. Intruders implant them on the user's computer to open remote access to it via FTP.
Server-Proxy	Proxy servers	They function as proxy servers. Intruders implant them on the user's computer to send spam under the user's name.
Server-Telnet	Telnet servers	They function as Telnet servers. Intruders implant them on the user's computer to open remote access to it via Telnet.
Server-Web	Web servers	They function as web servers. Intruders implant them on the user's computer to open remote access to it via HTTP.
RiskTool	Tools for working at a local computer	They provide the user with additional options when working at the user's own computer. The tools allow the user to hide files or windows of active applications and terminate active processes.
NetTool	Network tools	They provide the user with additional options when working with other computers on the network. These tools allow restarting them, detecting open ports, and starting applications that are installed on the computers.
Client-P2P	P2P network clients	They allow working on peer-to-peer networks. They can be used by intruders for spreading malware.
Client-SMTP	SMTP clients	They send email messages without the user's knowledge. Intruders implant them on the user's computer to send spam under the user's name.
WebToolbar	Web toolbars	They add toolbars to the interfaces of other applications to use search engines.
FraudTool	Pseudo-programs	They pass themselves off as other programs. For example, there are pseudo-anti-virus programs that display messages about malware detection. However, in reality, they do not find or disinfect anything.

- **Packed objects whose packing may be used to protect malicious code**

  Subcategory: Packed files that may cause harm.

  Danger level: Medium.

  The file is packed using a special packer that is used for packing malware: viruses, worms, Trojans. Kaspersky Industrial CyberSecurity for Nodes scans the unpacker module within SFX (self-extracting) archives.

  To hide malware from detection by an anti-virus, hackers pack it using special packers. Kaspersky experts have identified packers that are the most popular amongst hackers.

- **Multi-packed objects**

  Subcategory: Multi-packed files.

Danger level: Medium.

The file is packed with one or more packers three or more times.

To hide malware from detection by an anti-virus, hackers may pack a file multiple times. Kaspersky Industrial CyberSecurity for Nodes scans packed files.

4. Save your changes.

Editing the list of trusted applications

The *list of trusted applications* is a list of applications whose file and network activity (including malicious activity) and access to the system registry are not monitored by Kaspersky Industrial CyberSecurity for Nodes. By default, Kaspersky Industrial CyberSecurity for Nodes monitors objects that are opened, executed, or saved by any application process and controls the activity of all applications and network traffic that is generated by them. After an application is added to the list of trusted applications, Kaspersky Industrial CyberSecurity for Nodes stops monitoring the application's activity.

The difference between scan exclusions and trusted applications is that for exclusions Kaspersky Industrial CyberSecurity for Nodes does not scan files, while for trusted applications it does not control the initiated processes. If a trusted application creates a malicious file in a folder which is not included in scan exclusions, Kaspersky Industrial CyberSecurity for Nodes will detect the file and eliminate the threat. If the folder is added to exclusions, Kaspersky Industrial CyberSecurity for Nodes will skip this file.

For example, if you consider objects that are used by the standard Microsoft Windows Notepad application to be safe, meaning that you trust this application, you can add Microsoft Windows Notepad to the list of trusted applications so that the objects used by this application are not monitored. This will increase computer performance, which is especially important when using server applications.

In addition, certain actions that are classified by Kaspersky Industrial CyberSecurity for Nodes as suspicious may be safe within the context of the functionality of a number of applications. For example, the interception of text that is typed from the keyboard is a routine process for automatic keyboard layout switchers (such as Punto Switcher). To take account of the specifics of such applications and exclude their activity from monitoring, we recommend that you add such applications to the trusted applications list.

Trusted applications help to avoid compatibility issues between Kaspersky Industrial CyberSecurity for Nodes and other applications (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Industrial CyberSecurity for Nodes and by another anti-virus application).

At the same time, the executable file and process of the trusted application are still scanned for viruses and other malware. An application can be fully excluded from Kaspersky Industrial CyberSecurity for Nodes scanning by means of scan exclusions.

Kaspersky Industrial CyberSecurity for Nodes does not support trusted applications lists containing over 5000 objects.

How to add an application to the trusted list in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy window, select **Supplementary**.

4. In the **Trusted zone** block, click the **Settings** button.

5. In the window that opens, select the **Trusted applications** tab.

   This opens a window containing a list of trusted applications.

6. Select the **Do not check file backup operations** check box if you want to skip the scan of file read operations if such operations are performed by backup tools installed on the protected device.

7. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company. The lists of trusted applications in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted applications from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted applications of the parent policy is not possible

8. Select the **Allow editing of local trusted applications** check box if you want to enable the user to create a local list of trusted applications. This way, a user can create their own local list of trusted applications in addition to the general list of trusted applications generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.

   If the check box is cleared, the user can access only the general list of trusted applications generated in the policy. Also, if this check box is cleared, Kaspersky Industrial CyberSecurity for Nodes hides the consolidated list of trusted applications in the Application Console.

9. Select the **Do not check file activity of the specified processes** check box to skip the scan of file operations for trusted processes.

10. Click **Add** and select an action:

    - **Category**. You can group trusted applications into separate categories. To create a new category, enter the name of the category and add at least one trusted application to the category.
    - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new trusted application to the root of the list.
    - **New exclusion to selected category**. To add a new trusted application to a specific category, select a category.
    - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add applications from the list of predefined trusted applications.

11. In the window that opens, select the **Use full process path on disk to consider it trusted** check box and enter the path to the file to determine whether the process is trusted.

    Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

    > Kaspersky Industrial CyberSecurity for Nodes does not support the `%userprofile%` environment variable when generating a list of trusted applications in the Kaspersky Security Center console. To apply the entry to all user accounts, you can use the * character (for example, `C:\Users\*\Documents\File.exe`). Whenever you add a new environment variable, you need to restart the application.

12. Configure the advanced settings for the trusted application (see the table below).

13. Click **OK**.

    The new trusted application will be added to the list. You can exclude an application from the trusted zone at any time using the check box next to the object.

14. Save your changes.

How to add an application to the trusted list in the Kaspersky Security Center Web Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

4. Select the **Application settings** tab.
5. Go to **Supplementary** → **Trusted zone** and click the **Configure** button.
6. In the window that opens, select the **Trusted applications** tab.
7. Select the **Do not check file backup operations** check box if you want to skip the scan of file read operations if such operations are performed by backup tools installed on the protected device.
8. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company. The lists of trusted applications in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted applications from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted applications of the parent policy is not possible
9. Select the **Allow editing of local trusted applications** check box if you want to enable the user to create a local list of trusted applications. This way, a user can create their own local list of trusted applications in addition to the general list of trusted applications generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.

   If the check box is cleared, the user can access only the general list of trusted applications generated in the policy. Also, if this check box is cleared, Kaspersky Industrial CyberSecurity for Nodes hides the consolidated list of trusted applications in the Application Console.

10. Select the **Do not check file activity of the specified processes** check box to skip the scan of file operations for trusted processes.
11. Click **Add** and select an action:

    - **Category**. You can group trusted applications into separate categories. To create a new category, enter the name of the category and add at least one trusted application to the category.
    - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new trusted application to the root of the list.
    - **New exclusion to selected category**. To add a new trusted application to a specific category, select a category.
    - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add applications from the list of predefined trusted applications.

12. In the window that opens, select the **Use full process path on disk to consider it trusted** check box and enter the path to the file to determine whether the process is trusted.

    Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

    > Kaspersky Industrial CyberSecurity for Nodes does not support the `%userprofile%` environment variable when generating a list of trusted applications in the Kaspersky Security Center console. To apply the entry to all user accounts, you can use the * character (for example, `C:\Users\*\Documents\File.exe`). Whenever you add a new environment variable, you need to restart the application.

13. Configure the advanced settings for the trusted application (see the table below).

14. Click **OK**.

    The new trusted application will be added to the list. You can exclude an application from the trusted zone at any time using the check box in the **Action** column.

15. Save your changes.

How to add an application to the trusted list in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

   The **Configure Trusted zone settings** window opens.

2. In the **Exclusions** section, click the **Settings** button next to the **Trusted applications** block.

3. Click **Add** and select an action:

   - **Category**. You can group trusted applications into separate categories. To create a new category, enter the name of the category and add at least one trusted application to the category.
   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new trusted application to the root of the list.
   - **New exclusion to selected category**. To add a new trusted application to a specific category, select a category.
   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add applications from the list of predefined trusted applications.

4. Select a file from the list or enter the path to the executable file of the trusted application.

   Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

   > Kaspersky Industrial CyberSecurity for Nodes supports environment variables. At the same time Kaspersky Industrial CyberSecurity for Nodes converts the path in the local interface of the application. In other words, if you enter the file path `%userprofile%\Documents\File.exe`, a `C:\Users\Fred123\Documents\File.exe` record is added in local interface of the application for user Fred123. Accordingly, Kaspersky Industrial CyberSecurity for Nodes ignores the `File.exe` trusted program for other users. To apply the entry to all user accounts, you can use the `*` character (for example, `C:\Users\*\Documents\File.exe`).

Whenever you add a new environment variable, you need to restart the application.

5. Configure the advanced settings for the trusted application (see the table below).

6. Click **OK**.

   The new trusted application will be added to the list. You can exclude an application from the trusted zone at any time using the check box next to the object name.

7. Save your changes.

Trusted application settings

Parameter	Description
Use full process path on disk to consider it trusted	Kaspersky Industrial CyberSecurity for Nodes uses the full path to the file to determine whether the process is trusted.
Use process file hash to consider it trusted	Kaspersky Industrial CyberSecurity for Nodes uses the selected file's hash to determine the process's trust status. If the check box is cleared, the file hash is not used to determine the process's trust status.
Rule usage	You can configure a list of Kaspersky Industrial CyberSecurity for Nodes components that will not monitor the activity of a trusted application: • **Real-Time File Protection**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes excludes from scanning all files opened using a trusted application. This option is enabled by default. • **Registry Access Monitoring**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor changes to registry keys within the monitoring scope of the System Integrity Monitoring component that are made by a trusted application. By default, the functionality is disabled. • **Behavior Detection and Exploit Prevention**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the file and network activity of a trusted application in the operating system using the Anti-Cryptor and Exploit Prevention components. By default, the functionality is disabled. • **Interaction with AMSI Scanner component**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor requests from a trusted application to the AMSI Scanner component. By default, the functionality is disabled. • **File Integrity Monitor**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor changes made to files within the monitoring scope of the System Integrity Monitoring component by a trusted application. By default, the functionality is disabled. • **Endpoint Agent telemetry**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not send telemetry data regarding the activity of a trusted application. By default, the functionality is disabled. If this functionality is disabled, you can separately configure the sending of telemetry data regarding the management of a trusted application via the console by selecting the **Interception of console interactive input for Endpoint Agent telemetry** check box. • **Applications Launch Control**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the launch of a trusted application through the Applications Launch Control component. By default, the functionality is disabled. For predefined trusted applications, all functionalities are enabled by default, except for **Applications Launch Control**. If the Anomaly Detection using Sigma rules component is installed, the **Endpoint Agent telemetry** functionality will also be disabled by default.
Allow interaction with the application interface	Kaspersky Industrial CyberSecurity for Nodes blocks all attempts to manage application services from a remote computer. If the check box is selected, the remote access application is allowed to manage Kaspersky Industrial CyberSecurity for Nodes settings through the Kaspersky Industrial CyberSecurity for Nodes interface.
Do not monitor child application activity	Kaspersky Industrial CyberSecurity for Nodes will not monitor the file activity or network activity of applications that are started by this application. You can apply the exclusion recursively. In this case, the application does not monitor the activity of the entire chain of child applications.
Do not inherit restrictions from the parent process (application)	The restrictions configured for the parent process will not be applied by Kaspersky Industrial CyberSecurity for Nodes to a child process. The parent process is started by an application for which application rights and application network rules are configured.
Do not scan process memory	Kaspersky Industrial CyberSecurity for Nodes does not scan process memory.

Creating a local trusted zone

The user now can create their own local trusted zone for a specific computer. This way, the user can create their own local lists of scan exclusions and trusted applications in addition to the general trusted zone in a policy. An administrator can allow or block the use of local exclusions or local trusted applications in policy settings. To do so, use the **Allow use of local exclusions** and **Allow editing of local trusted applications** check boxes on the **Scan exclusions** and **Trusted applications** tabs in the **Trusted zone** section of the policy.

If creating a local trusted zone is allowed by an administrator, the user can add their own scan exclusions and trusted applications in the Application Console. At the same time, the user does not have permissions to modify or delete objects from the trusted zone configured in the policy. The administrator can also view, add, modify, or delete list items in the Kaspersky Security Center console if exclusions need to be added for an individual computer.

Kaspersky Industrial CyberSecurity for Nodes hides the lists of scan exclusions and trusted applications in the Application Console if configuration of the trusted zone is blocked by the administrator in the console ("closed lock" symbol) and local scan exclusions and trusted applications are prohibited.

How to add an object to the local trusted zone in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. In the computer properties window, select the **Applications** section.
5. In the list of Kaspersky applications installed on the computer, select **Kaspersky Industrial CyberSecurity for Nodes** and double-click to open the application properties.
6. In the application settings window, select **Supplementary** → **Trusted zone** and click **Settings**.
7. On the **Scan exclusions** tab, make a list of local scan exclusions.

   The rules for creating local scan exclusions are the same as for general exclusions. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:
8. On the **Trusted applications** tab, make a list of local trusted applications. This opens a window containing a list of local trusted applications.

   Rules for adding applications to the list of local trusted applications are the same as the rules for adding them to the general list. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:
9. Save your changes.

How to add an object to the local trusted zone in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
2. Click the name of the computer on which you want to allow a user to perform a blocked action.

3. Select the **Applications** tab.

4. Click **Kaspersky Industrial CyberSecurity for Nodes**.

   This opens the local application settings.

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

6. In the application settings window, select **Supplementary** → **Trusted zone** and click **Configure**.

   The **Exclusions and types of detected objects** window opens.

7. On the **Scan exclusions** tab, make a list of local scan exclusions.

   Rules for creating local exclusions are the same as the rules for creating general exclusions. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

8. On the **Trusted applications** tab, make a list of local trusted applications.

   Rules for adding applications to the list of local trusted applications are the same as the rules for adding them to the general list. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

9. Save your changes.

How to create a local scan exclusion in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

   The **Configure Trusted zone settings** window opens.

2. In the **Scan exclusions and trusted applications** section, click the **Settings** button next to the **Local scan exclusions** block.

   > Kaspersky Industrial CyberSecurity for Nodes hides the list of scan exclusions in the Application Console if configuration of scan exclusions is blocked by the administrator in the Kaspersky Security Center Administration Console ("closed lock" symbol) and local scan exclusions are prohibited (the **Allow use of local exclusions** check box is cleared).

3. Click **Add** and select an action:

   - **Category**. You can group scan exclusions into separate categories. To create a new category, enter the name of the category and add at least one scan exclusion to the category.
   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new scan exclusion to the root of the list.
   - **New exclusion to selected category**. To add a new scan exclusion to a specific category, select a category.
   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add exclusions from the list of predefined scan exclusions.

4. Selecting **New exclusion** opens the **Scan exclusion** window.

5. To exclude a file or folder from scan, select the **File or folder** check box. Click the **Select file or folder** link to open a window, and in that window, select a file or folder by clicking **Browse**.

You can also enter the path manually. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

- The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

- Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.

- The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

  You can use masks at the beginning, in the middle or at the end of the file path. For example, if you want to add a folder for all users to exclusions, enter the `?:\Users\*\Folder\` mask.

6. To exclude a predefined area from scan, select the **Predefined scope** check box. Click the **select predefined scope** link to open a window, and in that window, select one the standard scopes on the protected device.

7. To exclude the specific objects from scan, select the **Type of detected object** check box. Click the **enter object names** link, click the **Add** button, and in the displayed window, enter the name of the object type according to the Kaspersky Encyclopedia classification (for example, `Email-Worm`, `Rootkit`, or `RemoteAdmin`).

   You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, Kaspersky Industrial CyberSecurity for Nodes excludes `Client-IRC`, `Client-P2P` and `Client-SMTP` objects from scans.

8. To exclude an individual file from scan, select the **Object hash** check box. Click the **enter object hash** link to open a window, and in that window, enter a file hash.

   If the file is modified, the file hash will also be modified. If this happens, the modified file will not be added to exclusions.

9. In the **Rule usage scope** block, select the components that you want the scan exclusion to apply to.

10. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

11. Save changes to add the exclusion to the list. You can disable the exclusion at any time using the check box next to the object.

How to add an application to the list of local trusted applications in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

   The **Configure Trusted zone settings** window opens.

2. In the **Exclusions** section, click the **Settings** button next to the **Local trusted applications** block.

   Kaspersky Industrial CyberSecurity for Nodes hides the consolidated list of trusted applications in the Application Console if configuration of trusted applications is blocked by the administrator in the Kaspersky Security Center Administration Console ("closed lock" symbol) and local trusted applications are prohibited (the **Allow editing of local trusted applications** check box is cleared).

3. Click **Add** and select an action:

   - **Category**. You can group trusted applications into separate categories. To create a new category, enter the name of the category and add at least one trusted application to the category.
   - **New exclusion**. Kaspersky Industrial CyberSecurity for Nodes adds a new trusted application to the root of the list.
   - **New exclusion to selected category**. To add a new trusted application to a specific category, select a category.
   - **Select exclusion from list**. To quickly configure Kaspersky Industrial CyberSecurity for Nodes, you can add applications from the list of predefined trusted applications.

4. Selecting **New exclusion** opens the **Scan exclusion** window.

5. Select the **Use full process path on disk to consider it trusted** check box and enter the path to the executable file of the trusted application.

   Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask:

   Kaspersky Industrial CyberSecurity for Nodes supports environment variables. At the same time Kaspersky Industrial CyberSecurity for Nodes converts the path in the local interface of the application. In other words, if you enter the file path `%userprofile%\Documents\File.exe`, a `C:\Users\Fred123\Documents\File.exe` record is added in local interface of the application for user Fred123. Accordingly, Kaspersky Industrial CyberSecurity for Nodes ignores the `File.exe` trusted program for other users. To apply the entry to all user accounts, you can use the `*` character (for example, `C:\Users\*\Documents\File.exe`).

   Whenever you add a new environment variable, you need to restart the application.

6. In the trusted application properties window, configure the advanced settings.

7. Save changes to add the exclusion to the list.

Exporting and importing the trusted zone

A *trusted zone* is a system administrator-configured list of objects and applications that Kaspersky Industrial CyberSecurity for Nodes does not monitor when active. The trusted zone consists of the following lists: *scan exclusions* and *trusted applications*. Then you can modify the file to, for example, add a large number of exclusions of the same type. You can also use the export/import function to back up the list of exclusions and the list of trusted applications, or to migrate the lists to a different server.

The application uses XML format for exporting and importing the *list of exclusions* and trusted applications.

Kaspersky Industrial CyberSecurity for Nodes does not support exclusion lists and trusted applications lists containing over 5000 objects.

How to export and import the trusted zone in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Supplementary** → **Trusted zone** and click **Settings**.
4. To export the list of rules:
   a. Select the **Scan exclusions** tab.
   b. If you want to export the entire list, click the button and select **Export**.
   c. If you want to export only part of the list, follow these steps:
      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.
      2. Click the button and select **Export selected**.
   d. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.
      Kaspersky Industrial CyberSecurity for Nodes exports the list to the XML file.
5. To export the list of trusted applications:
   a. Select the **Trusted applications** tab.
   b. If you want to export the entire list, click the button and select **Export**.
   c. If you want to export only part of the list, follow these steps:
      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.
      2. Click the button and select **Export selected**.
   d. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.
      Kaspersky Industrial CyberSecurity for Nodes exports the list to the XML file.
6. To import the list of exclusions:
   a. Select the **Scan exclusions** tab.
      This opens a window containing a list of exclusions.
   b. Click on the folder icon and select **Import** from the drop-down list.
   c. In the window that opens, select the XML file from which you want to import the list of exclusions.

d. Open the file.

If the computer already has a list of exclusions, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

7. To import a list of trusted applications:

a. Select the **Trusted applications** tab.

This opens a window containing a list of trusted applications.

b. Click **Import**.

c. This opens a window; in that window, select the XML file from which you want to import the list of trusted applications.

d. Open the file.

If the computer already has a list of trusted applications, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

8. Save your changes.

How to export and import the trusted zone in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

The policy properties window opens.

3. Select the **Application settings** tab.
4. Go to **Supplementary** → **Trusted zone** and click the **Configure** button.
5. To export the list of rules:

a. On the **Scan exclusions and trusted applications** tab, select the exclusions that you want to export.

b. Click the three dots and select **Export**.

c. Confirm that you want to export only the selected exclusions, or export the entire list of exclusions.

Kaspersky Industrial CyberSecurity for Nodes exports the list to the XML file.

6. To export the list of trusted applications:

a. On the **Scan exclusions and trusted applications** tab, select the applications that you want to export.

b. Click the three dots and select **Export**.

c. Confirm that you want to export only the selected applications, or export the entire list.

Kaspersky Industrial CyberSecurity for Nodes exports the list to the XML file.

7. To import the list of exclusions:

    a. On the **Scan exclusions and trusted applications** tab, click **Import from the previous version** if you want to import the list of exclusions from an XML file created in version 4.0 or earlier of the application.

    If you are importing rules from an XML file created in version 4.5 or later, click **Import**.

    b. If the computer already has a list of exclusions, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

    c. In the window that opens, select the XML file from which you want to import the list of exclusions.

    d. Click **Import**.

8. To import a list of trusted applications:

    a. On the **Scan exclusions and trusted applications** tab, click **Import from the previous version** if you want to import the list of trusted applications from an XML file created in version 4.0 or earlier of the application.

    If you are importing trusted applications from an XML file created in version 4.5 or later, click **Import**.

    b. If the computer already has a list of trusted applications, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

    c. This opens a window; in that window, select the XML file from which you want to import the list of trusted applications.

    d. Click **Import**.

9. Save your changes.

How to export or import the trusted zone in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

    The **Configure Trusted zone settings** window opens.

2. To export the list of exclusions or trusted applications:

    a. In the **Exclusions** section, click the **Settings** button next to the **Scan exclusions** or **Trusted applications** blocks.

    This opens a window containing a list of scan exclusions or a list of trusted applications.

    b. If you want to export the entire list, click the button and select **Export**.

    c. If you want to export only part of the list, follow these steps:

        1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

        2. Click the button and select **Export selected**.

    d. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

    Kaspersky Industrial CyberSecurity for Nodes exports the list to the XML file.

3. To import a list of exclusions or trusted applications:

    a. In the **Exclusions** section, click the **Settings** button next to the **Scan exclusions** or **Trusted applications** blocks.

    b. Select the exclusions or trusted applications that you want to import.

    c. Click on the folder icon and select **Import**.

    d. This opens a window; in that window, select the XML file from which you want to import the list of exclusions or trusted applications.

    e. Open the file.

    If the computer already has a list of exclusions, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

4. Save your changes.

Using trusted system certificate storage

Use of system certificate storage lets you exclude applications signed by a trusted digital signature from virus scans. Kaspersky Industrial CyberSecurity for Nodes automatically assigns such applications to the *Trusted* group.

How to configure the use of a trusted system certificate storage in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Supplementary → Trusted zone** and click **Settings**.
4. Select the **Trusted system certificate store** tab.
5. Select the **Use trusted system certificate store** check box, and in the drop-down list, select the system store that you want Kaspersky Industrial CyberSecurity for Nodes to consider trusted.
6. Save your changes.

How to configure the use of a trusted system certificate storage in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

    The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Supplementary → Trusted zone** and click the **Configure** button.
5. Select the **Trusted system certificate store** tab.

6. Select the **Use trusted system certificate store** check box, and in the drop-down list, select the system store that you want Kaspersky Industrial CyberSecurity for Nodes to consider trusted.

7. Save your changes.

How to configure the use of a trusted system certificate storage in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Trusted zone** from the context menu of the node.

   The **Configure Trusted zone settings** window opens.

2. Under **Trusted system certificate store**, select the **Use trusted system certificate store** check box, and in the drop-down list, select the system store that you want Kaspersky Industrial CyberSecurity for Nodes to consider trusted.

3. Save your changes.

Predefined scan exclusions and trusted applications

Predefined scan exclusions and trusted applications let you quickly add processes and files of the following software to the trusted zone:

- Industrial software
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Hyper-V
- The data deduplication process in Microsoft Windows Server
- Microsoft System Center Configuration Manager

You can select predefined exclusions and trusted applications in the following ways:

- Installing the application.
  - Installing the application locally using the Wizard
  - Installation package properties
- Setting the policy.
  - New policy wizard
  - Policy properties: scan exclusions and trusted applications
  - On the command line.

Industrial software exclusion profiles

Exclusion profile is a set of exclusion rules in XML format intended to add processes and files of specific industrial applications to lists of trusted applications and scan exclusions, and also to configure the Applications Launch Control rules.

The table below lists all available industrial application exclusion profiles.

The rules for each exclusion profile assume that the industrial application is installed in the default folder. If an industrial application is installed in a folder other than the default folder, the rules of the corresponding exclusion profile must be adjusted manually after Kaspersky Industrial CyberSecurity for Nodes is installed.

Industrial software exclusion profiles

Exclusion profile	Trusted Zone configuration rules	Application Launch Control configuration rules	Exclusion profile name for the command line
ABB 800xA DCS	Yes	No	`ABB_800xA_DCS`
ABB MicroSCADA	Yes	No	`ABB_MicroSCADA`
AVADS Archiving Server 1.2	Yes	No	`AVADS_AS_1.2`
AVADS SAR Expert 1.0	Yes	No	`AVADS_SAR_Expert_1.0`
Bently Nevada System 1	Yes	Yes	`BakerHughes_BentlyNevadaSystem`
Bosch Building Integration System	Yes	No	`BOSCH_BIS`
BRIC	Yes	No	`BRIC_IDE`
Consen SC9000	Yes	No	`Consen`
Emerson DeltaV	Yes	Yes	`Emerson_DeltaV`
Emerson OpenEnterprise	Yes	Yes	`Emerson_OpenEnterprise`
Emerson Ovation	Yes	No	`Emerson_Ovation`
Emerson PipelineManager	Yes	No	`Emerson_Pipeline`
GE Cimplicity	Yes	No	`GE_Cimplicity`
Honeywell Experion PKS	Yes	No	`Honeywell_Experion_PKS`
MasterSCADA4D	Yes	No	`MasterSCADA4D`
Mitsubishi MAPS	Yes	No	`Mitsubishi_MAPS`
Nefteavtomatika "NaftaManagement PCM" 25.01	Yes	No	`Nefteavtomatika_NaftaManagement_PCM_25.01`
OMRON CX-Supervisor	Yes	No	`OMRON_CX-Supervisor`
PcVue Solutions 15	Yes	Yes	`PcVue_PcVue15`
RegLab PC "AstraRegul" 2025.08.15.00	Yes	No	`RegLab_AstraRegul_2025.08.15.00`
Rexroth IndraWorks	Yes	No	`Rexroth_IndraWorks`
Rockwell Automation FactoryTalk View	Yes	No	`Rockwell_Automation_FactoryTalk_View`
Schneider Electric Citect SCADA	Yes	No	`Schneider_Electric_Citect_SCADA`
Schneider Electric Clear SCADA	Yes	Yes	`Schneider_Electric_Clear_SCADA`

Exclusion profile	Trusted Zone configuration rules	Application Launch Control configuration rules	Exclusion profile name for the command line
Schneider Electric EcoStruxure Foxboro DCS	Yes	No	`Schneider_Electric_EcoStruxure_Foxboro_DCS`
Schneider Electric Unity Pro	Yes	No	`Schneider_Electric_Unity_Pro`
Siemens SIMATIC PCS 7 v8.2	Yes	No	`Siemens_SIMATICPCS7-8.2SP1`
Siemens SIMATIC PCS 7 v9.0	Yes	No	`Siemens_SIMATICPCS7-9.0SP2`
Siemens SIMATIC PCS 7 v9.1	Yes	Yes	`Siemens_SIMATICPCS7-9.1`
Siemens SIMATIC WinCC OA	Yes	Yes	`Siemens_SIMATIC_WinCC_OA`
Siemens SIMATIC WinCC	Yes	No	`Siemens_SIMATIC_WinCC`
Siemens SIMATIC STEP7	Yes	No	`Siemens_SIMATIC_STEP7`
Siemens TIA Portal	Yes	No	`Siemens_TIA_Portal`
Siemens DIGSI	Yes	No	`Siemens_DIGSI`
Siemens SICAM PAS	Yes	No	`Siemens_SICAM_PAS`
Valmet DNA	Yes	Yes	`Valmet_DNA`
Wonderware InTouch	Yes	No	`Wonderware_InTouch`
Wonderware System Platform 2017	Yes	No	`Wonderware_System-Platform-2017`
Yokogawa CENTUM VP	Yes	No	`Yokogawa_CENTUM_VP`
Yokogawa ProSafe-RS	Yes	No	`Yokogawa_ProSafe-RS`
Yokogawa FAST/TOOLS	Yes	No	`Yokogawa_FAST_TOOLS`
AVADS SAR Expert 1.0	Yes	No	`AVADS_SAR_Expert_1.0`
AVADS Archiving Server 1.2	Yes	No	`AVADS_AS_1.2`
AVM-Energo SCADA Sonica 7.90.26	Yes	No	`AVM_Energo_SCADA_Sonica_7.90.26`
Alpha.Platform	Yes	Yes	`AutomiqSoft_AlphaPlatform`
VACS	Yes	Yes	`SPEMT_VACSStandart`
GAUS	Yes	No	`GAUS`
ISUB ARBITER	Yes	No	`ARBITR`
Concor_SP KT	Yes	No	`Software_Platform_KT_1.2`
PK AstraRegul	Yes	No	`AstraRegul`
NaftaProcess DCS	Yes	Yes	`NaftaProcess_DCS`
Supcon_SP i-OMC	Yes	No	`SUPCON i-OMC_1.2`
Sib MIR Sibmir_SCADA 1.3	Yes	No	`SibMir_SCADA`
SimpLight_Linux SimpLight_Linux	Yes	No	`SIMP_Light`
TEKON	Yes	No	`TECON`
Tornado-N	Yes	Yes	`Tornado_Tornado-N`
TREI	Yes	No	`TREI`
CASCADE 3.18 Digital Platform	Yes	No	`Kaskad_3.18`
CASCADE 4 Digital Platform	Yes	No	`KASKAD_4.0`
EKRA (EKRASMS, EKRASMS-SP)	Yes	Yes	`EKRA`

To apply an industrial software exclusion profile during the installation of Kaspersky Industrial CyberSecurity for Nodes:

- Select the required exclusion profile at the corresponding step of the Setup Wizard.
- Enter the command line installation option: `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`.

Real-Time File Protection

The Real-Time File Protection component of Kaspersky Industrial CyberSecurity for Nodes scans the following protected device objects when they are accessed:

- Files
- NTFS alternate data streams.
- Master boot records and boot sectors on local hard drives and external devices.
- Windows Server 2016 and Windows Server 2019 container files.

When any application writes or reads a file on the protected device, Kaspersky Industrial CyberSecurity for Nodes intercepts the file, scans it for threats, and, if a threat is detected, performs a default action or an action you have specified: try to disinfect, move to Quarantine, or delete it. Before disinfection or deletion, Kaspersky Industrial CyberSecurity for Nodes saves an encrypted copy of the source file to the Backup folder.

Kaspersky Industrial CyberSecurity for Nodes intercepts file operations, executed in Windows Server 2016 and Windows Server 2019 containers.

A *container* is an isolated environment, which allows applications to run without direct interaction with the operating system. If container is located in the component protection scope, Kaspersky Industrial CyberSecurity for Nodes scans container files, which are being accessed by users, for computer threats. When a threat is detected, the application attempts to disinfect the container. If disinfection succeeds, the container continues to work. If disinfection fails, the container is turned off.

Kaspersky Industrial CyberSecurity for Nodes also detects malware for processes running under Windows Subsystem for Linux®. For such processes, the Real-Time File Protection component applies action defined by the current configuration.

About the task protection scope and security settings

By default, the Real-Time File Protection component protects all objects of the device file system. If there is no security requirement to protect all objects of the file system or you want to exclude any objects from the task scope, you can limit the protection scope.

In the Application Console, the protection scope is displayed as a list of the device's file resources that Kaspersky Industrial CyberSecurity for Nodes can monitor.

Security settings

The task security settings can be configured as common settings for all nodes or items included in the protection scope, or as different settings for each node or item in the device's file resource list.

Security settings configured for the selected parent node are automatically applied to all its child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected protection scope can be configured using one of the following methods:

- Selecting one of three predefined security levels.
- Configuring the security settings manually for the selected nodes or items in the file resource list (the security level changes to **Custom**).

Predefined protection scopes

The file resource list displays the nodes to which you have read-access based on the configured Microsoft Windows security settings.

Kaspersky Industrial CyberSecurity for Nodes covers the following predefined protection scopes:

- **Local hard drives**. Kaspersky Industrial CyberSecurity for Nodes protects files on the device hard drives.
- **Removable drives**. Kaspersky Industrial CyberSecurity for Nodes protects files on external devices, such as CDs or removable drives. All removable drives, individual disks, folders or files can be included in or excluded from the protection scope.
- **Network**. Kaspersky Industrial CyberSecurity for Nodes protects files that are written to network folders or read from them by applications running on the device. Kaspersky Industrial CyberSecurity for Nodes does not protect files when such files are accessed by applications from other protected devices.

By default, you can view and configure predefined protection scopes in the scope list; you can also add predefined scopes to the list during its formation in the protection scope settings.

Connected network drives will also not be displayed in the protected device's file resource list. To include objects on network drives in the protection scope, specify the path to the folder that corresponds to this network drive in UNC (Universal Naming Convention) format.

About predefined security levels

One of the following predefined security levels for the nodes selected either in the protected device's file resource tree or file resource list can be applied: **Maximum performance**, **Recommended**, **Maximum protection**, and **Inform**. Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if your network has additional protected device security measures, for example, firewalls and existing security policies, beyond using Kaspersky Industrial CyberSecurity for Nodes on protected devices and workstations.

Recommended

The **Recommended** security level ensures the best combination of protection and performance impact on devices. Kaspersky experts recommend this level as adequate to protect devices on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization's network has elevated device security requirements.

Inform

The **Inform** security level is recommended if there are potentially many infected computers in the corporate network and blocking them could significantly disrupt the operation of the organization.

Preset security levels and corresponding setting values

Options	Security level			
	Maximum performance	Recommended	Maximum protection	Inform
Objects protection	Objects scanned according to list of extensions specified in anti-virus database	Objects scanned by format	Objects scanned by format	Objects scanned by format
Scan only new and modified files	Enabled	Enabled	Disabled	Enabled
Scan of compound files	Disabled	Scan files in Microsoft Office formats	Scan files in Microsoft Office formats	Scan files in Microsoft Office formats
Action to perform on infected and other objects	Block access and disinfect. Remove, if disinfection fails	Block access and perform action recommended by Kaspersky experts	Block access and disinfect. Remove, if disinfection fails	Inform
Apply the action to the selected object types	Disabled	Disabled	Disabled	Disabled
Entirely remove the compound file that cannot be modified by the application in case of embedded object detection	Disabled	Disabled	Enabled	Disabled
System-critical objects are files required for the operation of the operating system and Kaspersky Industrial CyberSecurity for Nodes. These files can not be deleted. Processes associated with such objects cannot be terminated.				
Unpack in the background compound files larger than (MB)				
Stop scanning if it takes longer than (sec)	60 sec.	60 sec.	60 sec.	60 sec.
Do not scan compound objects larger than (MB)	8 MB	8 MB	Not set	8 MB

Options	Security level			
	Maximum performance	Recommended	Maximum protection	Inform
Use iSwift technology	Enabled	Enabled	Enabled	Enabled
Use iChecker technology	Enabled	Enabled	Enabled	Enabled

File extensions scanned by default by the Real-Time File Protection component

Kaspersky Industrial CyberSecurity for Nodes scans files with the following extensions by default:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*

- *emf;*
- *eml;*
- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*

- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*

- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Configuring Real-Time File Protection component

By default, the Real-Time File Protection component uses the settings described in the table below. You can change the values of these settings.

Real-Time File Protection component default settings

Parameter	Default value	Description
Protection scope	The entire protected device, excluding virtual drives.	Use this option to change the protection scope.
Security settings	Common settings for the entire protection scope correspond to the **Recommended** security level.	For nodes selected in the protected device's file resource list or tree, you can: • Select a different predefined security level • Manually change security settings You can save a group of security settings for a selected node as a template to use later for a different node.
Objects protection mode	**Smart mode**.	Use this option to select the protection mode, i.e. define the type of access attempts for which Kaspersky Industrial CyberSecurity for Nodes scans objects.
Heuristic analyzer	The **Medium** security level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level can be configured.
Block access to network shared resources for the sessions that show malicious activity	Not applied.	Use this option to block current session and to add host IP or host LUID for which malicious activity was detected in the Blocked hosts storage section.

Parameter	Default value	Description
Launch critical areas scan when active infection is detected	Applied.	When active infection is detected, Kaspersky Industrial CyberSecurity for Nodes creates and launches Critical Areas Scan task.
Stop the container if disinfection fails	Applied.	The application may not have sufficient read and write rights for the detected object. In that case, disinfecting or deleting the detected object is impossible. If this check box is selected, the application blocks the detected object and stops the container. If this check box is cleared, the application only blocks the detected object.
Do not scan file operations executed in Windows containers	Applied.	If the check box is selected, the application scans the container only at the container startup. If the check box is cleared, the application scans the container continuously in real time.

How to enable virus scans of files in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. In the **Real-Time File Protection settings** section, click **Settings**.
5. Select the **Real-Time File Protection** check box.
6. In the **Objects protection mode** block, on the **General** tab, select the Real-Time File Protection operation mode:
   - **Smart mode**. Kaspersky Industrial CyberSecurity for Nodes selects objects to be scanned on its own. An object is scanned on being opened and then again after being saved if the object has been modified. If the object is accessed multiple times and modified by the process, Kaspersky Industrial CyberSecurity for Nodes rescans the object only after the object is saved by the process for the last time.
   - **On access and modification**. Kaspersky Industrial CyberSecurity for Nodes scans an object when it is opened and rescans after it is saved, if the object was modified. This option is selected by default.
   - **On access**. Kaspersky Industrial CyberSecurity for Nodes scans all objects when they are opened for reading, execution, or modification.
   - **When run**. Kaspersky Industrial CyberSecurity for Nodes scans a file only when it is accessed to be executed.
7. Clear or select the **Use heuristic analysis** check box.
8. Select or clear the **Block access to network shared resources for the sessions that show malicious activity** check box.
9. Clear or select the **Launch critical areas scan when active infection is detected** check box.

   If the check box is selected, when active infection is detected, Kaspersky Industrial CyberSecurity for Nodes runs the predefined *Critical Areas Scan* task. The check box is selected by default.
10. Specify settings for scanning file operations executed in Windows containers.
11. Save your changes.

How to enable virus scans of files in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Real-Time File Protection** and click the **Configure** button.
5. Select the **Enable Real-Time File Protection** check box.
6. In the **Objects protection mode** block, on the **General** tab, select the Real-Time File Protection operation mode:

   - **Smart mode**. Kaspersky Industrial CyberSecurity for Nodes selects objects to be scanned on its own. An object is scanned on being opened and then again after being saved if the object has been modified. If the object is accessed multiple times and modified by the process, Kaspersky Industrial CyberSecurity for Nodes rescans the object only after the object is saved by the process for the last time.
   - **On access and modification**. Kaspersky Industrial CyberSecurity for Nodes scans an object when it is opened and rescans after it is saved, if the object was modified. This option is selected by default.
   - **On access**. Kaspersky Industrial CyberSecurity for Nodes scans all objects when they are opened for reading, execution, or modification.
   - **When run**. Kaspersky Industrial CyberSecurity for Nodes scans a file only when it is accessed to be executed.
7. Clear or select the **Use heuristic analysis** check box.
8. Select or clear the **Block access to network shared resources for the network sessions showing malicious activity** check box.
9. Clear or select the **Launch critical areas scan when active infection is detected** check box.

   If the check box is selected, when active infection is detected, Kaspersky Industrial CyberSecurity for Nodes runs the predefined *Critical Areas Scan* task. The check box is selected by default.
10. Specify settings for scanning file operations executed in Windows containers.
11. Save your changes.

How to enable virus scans of files in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection** → **Real-Time File Protection**.
2. In the results pane of the **Real-Time File Protection** node, click **Properties**.

   The **Properties: Real-Time File Protection** window opens.
3. Select the **Real-Time File Protection** check box.

4. In the **Objects protection mode** block, on the **General** tab, select the Real-Time File Protection operation mode:

   - **Smart mode**. Kaspersky Industrial CyberSecurity for Nodes selects objects to be scanned on its own. An object is scanned on being opened and then again after being saved if the object has been modified. If the object is accessed multiple times and modified by the process, Kaspersky Industrial CyberSecurity for Nodes rescans the object only after the object is saved by the process for the last time.

   - **On access and modification**. Kaspersky Industrial CyberSecurity for Nodes scans an object when it is opened and rescans after it is saved, if the object was modified. This option is selected by default.

   - **On access**. Kaspersky Industrial CyberSecurity for Nodes scans all objects when they are opened for reading, execution, or modification.

   - **When run**. Kaspersky Industrial CyberSecurity for Nodes scans a file only when it is accessed to be executed.

5. Clear or select the **Use heuristic analysis** check box.

6. Select or clear the **Block access to network shared resources for the sessions that show malicious activity** check box.

7. Clear or select the **Launch critical areas scan when active infection is detected** check box.

   If the check box is selected, when active infection is detected, Kaspersky Industrial CyberSecurity for Nodes runs the predefined *Critical Areas Scan* task. The check box is selected by default.

8. Specify settings for scanning file operations executed in Windows containers.

9. Save your changes.

Configuring the protection scope for the Real-Time File Protection component

By default, the Real-Time File Protection component uses common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for individual items in the device's file resource list.

If the same object is included in multiple protection scope entries and these entries have different security levels, the last rule in the list takes priority. For example, consider a protection scope that includes two entries: **All hard drives** (security level **Inform**) and `*\Users\*\Downloads\*` (security level **Custom**). The application scans hard drives in accordance with the Inform level, except the `Downloads` folder. The application scans the `Downloads` folder in accordance with manually specified settings because this entry is the last in the list of the protection scope.

How to configure the protection scope for Real-Time File Protection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. In the **Real-Time File Protection** section, click **Settings**.
5. Select the **Protection scope** tab.
6. In the list of file resource of the protected device, select items for which you want to set a predefined security level.
7. If the file share is not in the list, add it manually:
   a. Click **Add**.
   b. Use the folder tree to specify the path to the required object or enter the path in the **Object** field.
      If necessary, use special characters to enter the object path mask:
      - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
      - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.
      - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

      The **This PC** object in the list of file resources of the computer includes the following objects: **All hard drives**, **All network drives** and **All removable drives**.
   c. Click **OK**.
8. Make sure that the selected file resource is included in the protection scope.
9. Specify a predefined security level for the selected protection scope by clicking **Configure**. By default, the same security settings are applied to the whole protection scope. These settings correspond to the **Recommended** predefined security level. You can also edit the default security settings.
10. Save your changes.

How to configure the protection scope for Real-Time File Protection in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Real-Time File Protection** and click the **Configure** button.
5. Select the **Protection scope** tab.
6. In the list of file resource of the protected device, select items for which you want to set a predefined security level.
7. If the file share is not in the list, add it manually:

   a. Click **Add**.

   b. In the **Object type** list, select an option:

   For the **Mask** option, use special characters to enter the object path mask:

   - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
   - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.
   - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

   The **This PC** object in the list of file resources of the computer includes the following objects: **All hard drives**, **All network drives** and **All removable drives**.

   c. Click **OK**.
8. Make sure that the selected file resource is included in the protection scope by using the toggle switch next to the list item.
9. Specify a predefined security level for the selected protection scope by clicking **Edit**. By default, the same security settings are applied to the whole protection scope. These settings correspond to the **Recommended** predefined security level. You can also edit the default security settings.
10. Save your changes.

How to configure the protection scope for Real-Time File Protection in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection → Real-Time File Protection**.

2. In the results pane of the **Real-Time File Protection** node, click **Configure protection scope**.

   The **Properties: Real-Time File Protection** window opens.

3. In the list of file resource of the protected device, select items for which you want to set a predefined security level.

4. If the file share is not in the list, add it manually:

   a. Click **Add**.

   b. Use the folder tree to specify the path to the required object or enter the path in the **Object** field.

   If necessary, use special characters to enter the object path mask:

   - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

   - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.

   - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

   The **This PC** object in the list of file resources of the computer includes the following objects: **All hard drives**, **All network drives** and **All removable drives**.

   c. Click **OK**.

5. Make sure that the selected file resource is included in the protection scope.

6. Specify a predefined security level for the selected protection scope by clicking **Configure**. By default, the same security settings are applied to the whole protection scope. These settings correspond to the **Recommended** predefined security level. You can also edit the default security settings.

7. Save your changes.

Configuring security settings manually

By default Real-Time Computer Protection tasks use common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for individual items in the device's file resource list or nodes in the tree.

When working with the protected device's file resource tree, security settings that are configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

How to configure security settings manually in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. In the **Real-Time File Protection** section, click **Settings**.
5. In the **Real-Time File Protection** window, go to the **Protection scope** tab.
6. Select the resource whose security settings you want to configure.
7. Click **Configure**.
8. In the window that opens, select the required security level and click **Settings**.
9. On the **General** tab, specify the following settings:
   - Objects that should be included in the protection scope:
     - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.
     - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.
   - In the **Optimization** block, select or clear the Scan only new and modified files check box.
   - In the **Scan of compound files** section, specify the compound objects that you want to include in the scan scope:
     - Scan archives
     - Scan distribution packages
     - Scan files in Microsoft Office formats
     - Scan email format files

10. On the **Actions** tab, specify the following settings:

    - Select the action to be performed on infected and other detected objects:

        - Inform
        - Block
        - **Perform additional action**

          Select the action from the drop-down list:

            - **Disinfect**
            - **Disinfect. Delete if disinfection fails**
            - Delete
            - Recommended

    - Configure actions to be performed on objects depending on the type of object detected:

        a. Clear or select the Apply the action to the selected object types check box.

        b. Click **Settings** and select the types of objects to be detected.

    - Configure actions on compound files that are not available for modification: clear or select the Entirely remove the compound file that cannot be modified by the application in case of embedded object detection check box.

11. On the **Optimization** tab, specify the following settings:

    - Unpack in the background compound files larger than (MB)
    - Stop scanning if it takes longer than (sec)
    - Do not scan compound objects larger than (MB)
    - Use iSwift technology
    - Use iChecker technology

12. Save the new security settings.

How to configure security settings manually in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Real-Time File Protection** and click the **Configure** button.
5. Select the **Protection scope** tab.

6. Do one of the following:

   - Click the **Add** button to add a new rule and specify security settings for it.
   - Select an existing rule and click **Edit** button.

   The **Edit scope** window opens.

7. Set the toggle switch to **Active**.
8. Select a security level and specify security settings as necessary.
9. In the **Objects protection mode** section, select the type of the object that you want to include in the protection scope:

   - Objects that should be included in the protection scope:
     - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.
     - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.

10. In the **Optimization** section, select or clear the **Protect only new and modified files** check box.
11. In the **Compound objects protection** section, specify the compound objects that you want to include in the scan scope:

    - **Scan archives**
    - **Scan distribution packages**
    - **Scan files in Microsoft Office formats**
    - **Scan email format files**

12. Select the action to be performed on infected and other detected objects:

    - **Inform**
    - **Block**
    - **Perform additional action**

      Select the action from the drop-down list:

      - **Disinfect**
      - **Disinfect, delete if disinfection fails**

- Delete
- Recommended

13. Configure actions to be performed on objects depending on the type of object detected:

    a. Clear or select the Apply the action to the selected object types check box.

    b. If the check box is selected, click **Settings** and select the types of objects to be detected.

14. Configure actions on compound files that are not available for modification: clear or select the Entirely remove the compound file that cannot be modified by the application in case of embedded object detection check box.

15. In the **Optimization** section, configure the following settings:

    - Unpack compound files in the background
    - Stop scanning if it takes longer than (sec)
    - Do not scan compound objects larger than (MB)
    - Use iSwift technology
    - Use iChecker technology

16. Save the new security settings.

How to configure security settings manually in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection** → **Real-Time File Protection**.

2. In the results pane of the **Real-Time File Protection** node, click **Configure protection scope**.

   The **Properties: Real-Time File Protection** window opens.

3. Select the resource whose security settings you want to configure.

4. Click **Configure**.

5. In the window that opens, select the required security level and click **Settings**.

6. On the **General** tab, specify the following settings:

    - Objects that should be included in the protection scope:

        - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.

        - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.

- **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.

- **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.

- In the **Optimization** block, select or clear the **Protect only new and modified files** check box.

- In the **Scan of compound files** section, specify the compound objects that you want to include in the scan scope:

  - **Scan archives**. Scanning ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE, and other archives. The application scans archives not only by extension, but also by format. When checking archives, the application performs a recursive unpacking. This allows the detection of threats inside multi-level archives (an archive within an archive).

  - **Scan distribution packages**. This check box enables/disables scanning of third-party distribution packages.

  - **Scan files in Microsoft Office formats**. Scans Microsoft Office files (DOC, DOCX, XLS, PPT and other Microsoft extensions). Office format files include OLE objects as well. Kaspersky Industrial CyberSecurity for Nodes scans office format files that are smaller than 1 MB, regardless of whether the check box is selected or not.

  - **Scan email format files**.

7. On the **Actions** tab, specify the following settings:

- Select the action to be performed on infected and other detected objects:

  - **Inform**

  - **Block**

  - **Perform additional action**.

    Select the action from the drop-down list:

    - **Disinfect**

    - **Disinfect. Delete if disinfection fails**

    - **Delete**

    - **Recommended**

- Configure actions to be performed on objects depending on the type of object detected:

  a. Clear or select the **Apply the action to the selected object types** check box.

  b. Click **Settings** and select the types of objects to be detected.

- Configure actions on compound files that are not available for modification: clear or select the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** check box.

8. On the **Optimization** tab, specify the following settings:

   - **Unpack in the background compound files larger than (MB)**
   - **Stop scanning if it takes longer than (sec)**
   - **Do not scan compound objects larger than (MB)**
   - **Use iSwift technology**
   - **Use iChecker technology**

9. Save the new security settings.

Container Scan

A *container* is an isolated environment in which an application can run without directly interacting with the operating system. Using containers involves the following risks:

- Hackers may be able to exploit containerization vulnerabilities to compromise applications inside the container.
- Hackers may exploit an insecure configuration of the container environment to gain unauthorized access to data on the computer or to compromise the integrity of the system.
- A successful attack on a container can allow a hacker to gain access to data on the computer.
- Hackers may exploit network vulnerabilities to intercept network traffic.

Kaspersky Industrial CyberSecurity for Nodes is an external tool for detecting malicious activity inside containers. This allows maintaining the performance of containers and prevents conflicts with other applications inside the container. Installing Kaspersky Industrial CyberSecurity for Nodes inside the container is not supported.

In addition to providing container security, Kaspersky Industrial CyberSecurity for Nodes allows managing applications inside containers using the Applications Launch Control component. The Applications Launch Control component is configured for containers in the same way as for applications installed on the computer. The System Integrity Monitoring component also supports containers.

Container requirements

- The container must be a Docker container. Other containerization tools are not supported.
- The container must run in process isolation mode. The Hyper-V isolation mode is not supported.
- The container must be placed on a Windows Server 2016, 2019, or 2022 server (Docker Host).
- The container must include a Windows image (Docker Image). Windows 10 and 11 are not supported. Linux images are not supported.
- Scanning containers running in WSL2 – Windows Subsystem for Linux v2 (Docker Wine) mode is not supported.

Action on threat detection

If a threat is detected inside a container, the application applies the action selected for the Real-Time File Protection component. The container scan has additional settings (see the instructions below). If a threat is detected, the application blocks the malicious activity and performs the selected action (for example, attempts to disinfect the object). Kaspersky Industrial CyberSecurity for Nodes can stop the container if it fails to disinfect the detected object. By default, container stopping is enabled.

How to configure scan of containers in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. In the **Real-Time File Protection** section, click **Settings**.
5. In the **Scan of file operations executed in Windows containers** block, configure the container scan settings:
   - **Stop the container if disinfection fails**. The application may not have sufficient read and write rights for the detected object. In that case, disinfecting or deleting the detected object is impossible. If this check box is selected, the application blocks the detected object and stops the container. If this check box is cleared, the application only blocks the detected object.
   - **Do not scan file operations executed in Windows containers**. If the check box is selected, the application scans the container only at the container startup. If the check box is cleared, the application scans the container continuously in real time.
6. Save the new security settings.

How to configure scan of containers in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Real-Time File Protection** and click the **Configure** button.
5. In the **Scan of file operations executed in Windows containers** block, configure the container scan settings:
   - **Stop the container if disinfection fails**. The application may not have sufficient read and write rights for the detected object. In that case, disinfecting or deleting the detected object is impossible. If this check box is selected, the application blocks the detected object and stops the container. If this check box is cleared, the application only blocks the detected object.
   - **Do not scan file operations executed in Windows containers**. If the check box is selected, the application scans the container only at the container startup. If the check box is cleared, the application scans the container continuously in real time.
6. Save the new security settings.

How to configure scan of containers in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection → Real-Time File Protection**.

2. In the results pane of the **Real-Time File Protection** node, click **Properties**.

   The **Properties: Real-Time File Protection** window opens.

3. In the **Scan of file operations executed in Windows containers** block, configure the container scan settings:

   - **Stop the container if disinfection fails**. The application may not have sufficient read and write rights for the detected object. In that case, disinfecting or deleting the detected object is impossible. If this check box is selected, the application blocks the detected object and stops the container. If this check box is cleared, the application only blocks the detected object.

   - **Do not scan file operations executed in Windows containers**. If the check box is selected, the application scans the container only at the container startup. If the check box is cleared, the application scans the container continuously in real time.

4. Save your changes.

KSN Usage

To protect your computer more effectively, Kaspersky Industrial CyberSecurity for Nodes uses data that is received from users around the globe. Kaspersky Security Network is designed for obtaining this data.

KSN functionality may not be available in the application in the U.S.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Industrial CyberSecurity for Nodes to new threats, improves the performance of some protection components, and reduces the likelihood of false positives. If you are participating in Kaspersky Security Network, KSN services provide Kaspersky Industrial CyberSecurity for Nodes with information about the reputation of scanned web addresses, as well as information about the category and reputation of scanned files. For more details on configuring access to KSN, refer to the Kaspersky Security Center Help.

Use of Kaspersky Security Network is voluntary. The application prompts you to use KSN during initial configuration of the application. Users can begin or discontinue participation in KSN at any time.

For more detailed information about sending Kaspersky statistical information that is generated during participation in KSN, and about the storage and destruction of such information, please refer to the Kaspersky Security Network Statement and the Kaspersky website. The ksn_<language ID>.txt file with the text of the Kaspersky Security Network Statement is included in the application distribution kit.

The infrastructure of Kaspersky reputation databases

Kaspersky Industrial CyberSecurity for Nodes supports the following infrastructure solutions for working with Kaspersky reputation databases:

- *Kaspersky Security Network (KSN)* is the solution that is used by most Kaspersky applications. KSN participants receive information from Kaspersky and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases.

- *Kaspersky Private Security Network (KPSN)* is a solution that enables users of computers hosting Kaspersky Industrial CyberSecurity for Nodes or other Kaspersky applications to obtain access to Kaspersky reputation databases, and to other statistical data without sending data to Kaspersky from their own computers. KPSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

  - Local workstations are not connected to the Internet.

  - Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

Enabling the use of Kaspersky Security Network

How to enable the use of Kaspersky Security Network.in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Network Administration Console tree, select the **Policies** folder.
2. Select the necessary policy of Kaspersky Industrial CyberSecurity for Nodes and double-click to open the policy properties.
3. This opens a window; in that window, in the list of sections, select **Real-Time Computer Protection → KSN Usage**.
4. Click **Settings**.
5. Select the **Kaspersky Security Network** check box to enable the component.

   If you enabled the use of KSN, Kaspersky Industrial CyberSecurity for Nodes will display the Kaspersky Security Network Statement. Please read and accept the Kaspersky Security Network (KSN) Statement terms of use if you agree to them.

   By default, Kaspersky Industrial CyberSecurity for Nodes uses the Extended mode of Kaspersky Security Network. The Extended Kaspersky Security Network mode is a mode in which Kaspersky Industrial CyberSecurity for Nodes sends additional data to Kaspersky.
6. If necessary, clear the **Enable extended KSN mode** check box.
7. Save your changes.

If the use of Kaspersky Security Network is enabled, Kaspersky Industrial CyberSecurity for Nodes uses information about the reputation of files, web resources, and applications received from Kaspersky Security Network.

How to enable the use of Kaspersky Security Network in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Kaspersky Security Network** child node.
3. In the main application window, click **Properties**.
4. Select the **Kaspersky Security Network** check box to enable the component.

   If you enabled the use of KSN, Kaspersky Industrial CyberSecurity for Nodes will display the Kaspersky Security Network Statement. Please read and accept the Kaspersky Security Network (KSN) Statement terms of use if you agree to them.

   By default, Kaspersky Industrial CyberSecurity for Nodes uses the Extended mode of Kaspersky Security Network. The Extended Kaspersky Security Network mode is a mode in which Kaspersky Industrial CyberSecurity for Nodes sends additional data to Kaspersky.
5. If necessary, clear the **Enable extended KSN mode** check box.
6. Save your changes.

If the use of Kaspersky Security Network is enabled, Kaspersky Industrial CyberSecurity for Nodes uses information about the reputation of files, web resources, and applications received from Kaspersky Security Network.

How to enable the use of Kaspersky Security Network in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Real-Time Computer Protection** → **KSN Usage** section and click the **Configure** button.
5. In the displayed window, select the **Enable Kaspersky Security Network** check box to enable the component.

   If you enabled the use of KSN, Kaspersky Industrial CyberSecurity for Nodes will display the Kaspersky Security Network Statement. If you agree, accept the Kaspersky Security Network terms of use.

   By default, Kaspersky Industrial CyberSecurity for Nodes uses the Extended mode of Kaspersky Security Network. The Extended Kaspersky Security Network mode is a mode in which Kaspersky Industrial CyberSecurity for Nodes sends additional data to Kaspersky.
6. If necessary, clear the **Enable extended KSN mode** check box.
7. Save your changes.

As a result, if the use of Kaspersky Security Network is enabled, Kaspersky Industrial CyberSecurity for Nodes uses information about the reputation of files, web resources, and applications received from Kaspersky Security Network.

Kaspersky Security Network usage statistics

While the *KSN Usage* task is running, you can view real-time information about the number of objects processed by Kaspersky Industrial CyberSecurity for Nodes from the moment when the task was started up until now.

To view KSN usage statistics:

1. In the Application Console tree, select the **Real-Time Computer Protection** section.
2. Select the **Kaspersky Security Network** child node.

   In the results pane, in the **Statistics** section, the task statistics is displayed (see the table below).

KSN statistics

Field	Description
File requests sent	Number of object reputation queries sent by Kaspersky Industrial CyberSecurity for Nodes to KSN.
Files untrusted in KSN	Number of objects with an untrusted reputation assigned by KSN.
Request sending errors	Number of KSN requests processed with an error.
Statistics formed	Number of generated statistic packages sent to KSN.
Objects removed	Number of objects successfully deleted by Kaspersky Industrial CyberSecurity for Nodes.

Field	Description
Objects not removed	Number of objects that Kaspersky Industrial CyberSecurity for Nodes attempted to delete unsuccessfully, because, for example, access to the object was blocked by another application.
Moved to Backup	Number of objects successfully copied to backup by Kaspersky Industrial CyberSecurity for Nodes.
Objects not moved to Backup	Number of objects that Kaspersky Industrial CyberSecurity for Nodes could not copy to backup, for example due to insufficient disk space. The application does not disinfect or delete files that it could not move to Backup.
Limited mode	The status signifies whether the application sends file reputation requests in a limited mode. In a limited mode Kaspersky Industrial CyberSecurity for Nodes sends only a part of file reputation requests according to Kaspersky experts recommendation.

Values of the **Objects removed**, **Objects not removed**, **Moved to Backup**, **Objects not moved to Backup** fields are generated from the statistics of the Real-Time File Protection component.

Limitations of Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) is a solution that enables users of computers hosting Kaspersky Industrial CyberSecurity for Nodes or other Kaspersky applications to obtain access to Kaspersky reputation databases, and to other statistical data without sending data to Kaspersky from their own computers. Kaspersky Private Security Network lets you use your own local reputation database to check the reputation of objects (files or web addresses). The reputation of an object added to the local reputation database has a higher priority than one added to KSN/KPSN. For example, imagine that Kaspersky Industrial CyberSecurity for Nodes is scanning a computer and requests the reputation of a file in KSN/KPSN. If the file has an *Untrusted* reputation in the local reputation database but has a *Trusted* reputation in KSN/KPSN, Kaspersky Industrial CyberSecurity for Nodes will detect the file as *Untrusted* and will take the action defined for detected threats.

However, in some cases Kaspersky Industrial CyberSecurity for Nodes might not request the reputation of an object in KSN/KPSN. If this is the case, Kaspersky Industrial CyberSecurity for Nodes will not receive data from the local reputation database of KPSN. Kaspersky Industrial CyberSecurity for Nodes might not request the reputation of an object in KSN/KPSN for the following reasons:

- Kaspersky applications are using offline reputation databases. Offline reputation databases are designed to optimize resources during operation of Kaspersky applications and to protect critically important objects on the computer. Offline reputation databases are created by Kaspersky experts based on data from Kaspersky Security Network. Kaspersky applications update offline reputation databases with anti-virus databases of the specific application. If offline reputation databases contain information about an object being scanned, the application does not request the reputation of this object from KSN/KPSN.

- Scan exclusions (trusted zone) are configured in the application settings. If this is the case, the application does not take into account the reputation of the object in the local reputation database.

- The application uses scan optimization technologies, such as iSwift or iChecker, or is caching reputation requests to KSN/KPSN. If this is the case, the application might not request the reputation of previously scanned objects.

- To optimize its workload, the application scans files of a certain format and size. The list of relevant formats and size limits are determined by Kaspersky experts. This list is updated with the application's anti-virus databases.

KSN Proxy settings

User computers managed by Kaspersky Security Center Administration Server can interact with KSN via the KSN Proxy service.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN even without direct access to the Internet.
- The KSN Proxy service caches processed data, thereby reducing the load on the external network communication channel and speeding up receipt of the information that is requested by the user's computer.

By default, after KSN is enabled and the KSN Statement is accepted, the application uses a proxy server to connect to Kaspersky Security Network. The proxy server used by the application is the Kaspersky Security Center Administration Server via TCP port 13111. Thus, if KSN Proxy is unavailable, you must check the operation of the device as a KSN proxy server. You must check the following:

- The *ksnproxy* service is running on the Administration Server.
- The Firewall on the computer is not blocking port 13111.

You can configure the use of KSN Proxy as follows: enable or disable KSN Proxy, and configure the port for the connection. To do so, you need to open the Administration Server properties. For details on KSN Proxy configuration, please refer to the Kaspersky Security Center Help. You can also enable or disable KSN Proxy for individual computers in the Kaspersky Industrial CyberSecurity for Nodes policy.

How to enable KSN Proxy in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy of Kaspersky Industrial CyberSecurity for Nodes and double-click to open the policy properties.
3. This opens a window; in that window, in the list of sections, select **Real-Time Computer Protection → KSN Usage**.
4. Click **Settings**.
5. In the **KSN Proxy Settings** block, use the **Use Administration Server as a KSN proxy server** check box to enable or disable KSN Proxy.
6. If necessary, select the **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** check box.

   If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes uses KSN servers when the KSN Proxy service is unavailable. KSN servers may be located both on the side of Kaspersky and on the side of third parties (when Kaspersky Private Security Network is used).
7. Save your changes.

How to enable KSN Proxy in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Kaspersky Security Network** child node.
3. In the main application window, click **Properties**.
4. In the **KSN Proxy Settings** block, use the **Use Administration Server as a KSN proxy server** check box to enable or disable KSN Proxy.
5. If necessary, select the **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** check box.

   If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes uses KSN servers when the KSN Proxy service is unavailable. KSN servers may be located both on the side of Kaspersky and on the side of third parties (when Kaspersky Private Security Network is used).
6. Save your changes.

How to enable KSN Proxy in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **KSN Usage** and click the **Configure** button.
5. Select or clear the **Use Administration Server as a KSN proxy server** check box to enable or disable KSN Proxy.
6. If necessary, select the **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** check box.

   If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes uses KSN servers when the KSN Proxy service is unavailable. KSN servers may be located both on the side of Kaspersky and on the side of third parties (when Kaspersky Private Security Network is used).
7. Save your changes.

The KSN Proxy address matches the Administration Server address. When the Administration Server domain name is changed, you need to manually update the KSN Proxy address.

Exploit Prevention

Kaspersky Industrial CyberSecurity for Nodes provides the ability to protect process memory from exploits. This functionality is implemented by the Exploit Prevention component which you can use to change the activity status of the component and configure the protection of processes from exploits.

The Exploit Prevention component detects program code that takes advantage of vulnerabilities on a computer to exploit administrator privileges or to perform malicious activities. For example, exploits can utilize a buffer overflow attack. To do so, the exploit sends a large amount of data to a vulnerable application. When processing this data, the vulnerable application executes malicious code. As a result of this attack, the exploit can start an unauthorized installation of malware. When there is an attempt to run an executable file from a vulnerable application that was not performed by the user, Kaspersky Industrial CyberSecurity for Nodes blocks this file from running or notifies the user. The component protects process memory from exploits by inserting an external Process Protection Agent in the protected process.

A *Process Protection Agent* (hereinafter also referred to as *Agent*) is a dynamically loaded Kaspersky Industrial CyberSecurity for Nodes module that is inserted in protected processes to monitor their integrity and reduce the risk of being exploited.

The Agent's operation within the protected process requires starting and stopping the process: the initial loading of the Agent into a process added to the protected process list is only possible if the process is restarted. Additionally, after a process has been removed from the protected process list, the Agent can be unloaded only after the process has been restarted.

The Agent must be stopped to unload it from protected processes: if the Exploit Prevention component is uninstalled, the application freezes the environment and forces the Agent to be unloaded from protected processes. If during uninstallation of the component Agent is inserted in any of the protected processes, you must terminate the affected process. A protected device restart may be required (for example, if system process is being protected).

If evidence of an exploit attack in a protected process is detected, Kaspersky Industrial CyberSecurity for Nodes performs one of the following actions:

- Terminates the process if an exploit attempt is made.
- Reports the fact that the process has been compromised.

You can stop process protection using one of the following methods:

- Uninstalling the component.
- Removing the process from the list of protected processes and restarting the process.

Exploit Prevention mode

You can select one of the following modes to configure actions taken to reduce risks that vulnerabilities will be exploited in protected processes:

- **Block**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes terminates a protected process upon detecting an exploit attempt if an active impact reduction technique has been applied to the process.

  Upon detecting an attempt to exploit a vulnerability in a protected critical operating system process, Kaspersky Industrial CyberSecurity for Nodes does not terminate the process, regardless of the mode indicated in the Exploit Prevention component settings.

- **Inform** (when working in the Kaspersky Security Center Web Console – **Inform**). Apply this mode to receive information about instances of exploits in protected processes using events in the Security log. The abused process continues to run.

  If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes creates events to log all attempts to exploit vulnerabilities. Selected by default.

Enabling and disabling Exploit Prevention

Kaspersky Industrial CyberSecurity for Nodes allows monitoring executable files being run by vulnerable applications. If Kaspersky Industrial CyberSecurity for Nodes detects that an executable file from a vulnerable application was run by something other than the user, Kaspersky Industrial CyberSecurity for Nodes will perform the selected action (for example, will block the operation).

How to enable or disable Exploit Prevention in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy of Kaspersky Industrial CyberSecurity for Nodes and double-click to open the policy properties.
3. This opens a window; in that window, in the list of sections, select **Real-Time Computer Protection → Exploit Prevention**.
4. Click **Settings**.
5. Select the **Exploit Prevention** check box to enable the component.
6. On the **General** tab, select an exploit prevention mode: **Block** or **Inform**.
7. If necessary, clear the **Exploit Prevention** check box to disable the component.
8. Save your changes.

How to enable or disable Exploit Prevention in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Exploit Prevention** child node.
3. In the main application window, click **Properties**.
4. Select the **Exploit Prevention** check box to enable the component.
5. On the **General** tab, select an exploit prevention mode: **Block** or **Inform**.
6. If necessary, clear the **Exploit Prevention** check box to disable the component.
7. Save your changes.

How to enable or disable Exploit Prevention in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Exploit Prevention** and click the **Configure** button.
5. This opens a window; in that window, under **Exploit Prevention mode**, select the **Prevent vulnerable processes exploit** check box to enable the component.
6. Select an exploit prevention mode: **Block** or **Inform**.
7. If necessary, clear the **Prevent vulnerable processes exploit** check box to disable the component.
8. Save your changes.

Enabling and disabling memory protection

Kaspersky Industrial CyberSecurity for Nodes blocks external processes that attempt to gain access to system processes. By default, protection of system process memory is enabled.

How to enable or disable memory protection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy of Kaspersky Industrial CyberSecurity for Nodes and double-click to open the policy properties.
3. This opens a window; in that window, in the list of sections, select **Real-Time Computer Protection** → **Exploit Prevention**.
4. Click **Settings**.

5. On the **General** tab, select the **Enable system process memory protection** check box.
6. If necessary, clear the **Enable system process memory protection** check box.
7. Save your changes.

How to enable or disable memory protection in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Exploit Prevention** child node.
3. In the main application window, click **Properties**.
4. On the **General** tab, select the **Enable system process memory protection** check box.
5. If necessary, clear the **Enable system process memory protection** check box.
6. Save your changes.

How to enable or disable memory protection in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Exploit Prevention** and click the **Configure** button.
5. In the window that opens, in the **System processes memory protection** block, select the **System processes memory protection** check box.
6. If necessary, clear the **System processes memory protection** check box to disable system process memory protection.
7. Save your changes.

Creating the list of protected processes

By default, the Exploit Prevention component protects multiple processes. The application can generate the list of protected processes automatically. You can also add or remove processes manually.

How to manage the list of protected processes in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy of Kaspersky Industrial CyberSecurity for Nodes and double-click to open the policy properties.
3. This opens a window; in that window, in the list of sections, select **Real-Time Computer Protection** → **Exploit Prevention**.

4. Click **Settings**.

5. On the **Protected processes** tab, select one of the following options to protect processes from malicious code injection:

   - **Automatically detect protected processes**. If you select this option, the application automatically creates a list of protected processes.

   - **Protect only processes from the list below**. If you select this option, you can select processes that you want to be protected.

6. If you selected **Protect only processes from the list below**, you can edit the list of protected processes by doing one of the following:

   - If necessary, click **Add** and select a process that you want to add to the list of protected processes.

   - If you want to delete a process from the created list of protected processes, select the process in the list and click **Delete**.

     The **Delete** button becomes available after you select one or more processes in the list.

7. Save your changes.

How to manage the list of protected processes using Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.

2. Select the **Exploit Prevention** child node.

3. In the main application window, click **Properties**.

4. On the **Protected processes** tab, select one of the following options to protect processes from malicious code injection:

   - **Automatically detect protected processes**. If you select this option, the application automatically creates a list of protected processes.

   - **Protect only processes from the list below**. If you select this option, you can select processes that you want to be protected.

5. If you selected **Protect only processes from the list below**, you can edit the list of protected processes by doing one of the following:

   - If necessary, click **Add** and select a process that you want to add to the list of protected processes.

   - If you want to delete a process from the created list of protected processes, select the process in the list and click **Delete**.

     The **Delete** button becomes available after you select one or more processes in the list.

6. Save your changes.

How to manage the list of protected processes in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Real-Time Computer Protection** → **Exploit Prevention** section and click the **Configure** button.
5. Under **Protected processes list**, select one of the following options to protect processes from malicious code injection:

   - **Automatically detect protected processes**. If you select this option, the application automatically creates a list of protected processes.
   - **Protect only processes from the list below**. If you select this option, you can add, edit, and remove processes that you want to be protected.
6. If you selected **Protect only processes from the list below**, do one of the following:

   - Click **Add** to open the **Protected process** window, and in that window:

     a. Select the **Protected process** check box.

     b. In the **Process name** field, enter the name of the process.

     c. Save your changes.
   - If necessary, edit process settings in the list of protected processes. To do this, perform the following actions:

     a. Select a process in the list of protected processes.

     b. Click **Edit**. The **Edit** button becomes available after you select one or more processes in the list.

     c. In the **Protected process** window, select or clear the **Protected process** check box.

     d. If necessary, edit the name of the process in the **Process name** field.

     e. Save your changes.
   - If necessary, you can remove a process from the list of protected processes. To do this, perform the following actions:

     a. Select one or more processes in the list of protected processes.

     b. Click **Delete**. The **Delete** button becomes available after you select one or more processes in the list.
7. Save your changes.

Remediation Engine

The Remediation Engine lets Kaspersky Industrial CyberSecurity for Nodes roll back actions that have been performed by malware in the operating system.

When rolling back malware activity in the operating system, Kaspersky Industrial CyberSecurity for Nodes performs the following actions:

- **File activity**
  - Deletes executable files that were created by malware on all media except network drives.
  - Deletes executable files that were created by programs that have been infiltrated by malware.
  - Restores files that have been modified or deleted by malware.

  The file recovery feature has a **number of limitations**.
  - The application restores files only on devices that have the NTFS or FAT32 file system.
  - The application can restore files with the following extensions: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
  - It is not possible to restore files residing on network drives or on rewritable CD/DVD discs.
  - It is not possible to restore files that were encrypted with the Encryption File System (EFS). For more details on EFS operation, please visit the Microsoft website.
  - The application does not monitor modifications to files performed by processes at the level of the operating system kernel.
  - The application does not monitor modifications made to files over a network interface (for example, if a file is stored in a shared folder and a process is started remotely from another computer).
- **Registry activity**
  - Deletes registry keys that were created by malware.

  Kaspersky Industrial CyberSecurity for Nodes does not restore registry keys that have been modified or deleted by malware.
- **System activity**
  - Terminates processes that have been initiated by malware.
  - Terminates processes into which a malicious application has penetrated.

  Kaspersky Industrial CyberSecurity for Nodes does not resume processes that have been halted by malware.

- **Network activity**
  - Blocks the network activity of malware.
  - Blocks the network activity of processes that have been infiltrated by malware.

A rollback of a malicious application's actions can be initiated by the Real-Time File Protection component or during an On-Demand Scan.

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

How to enable or disable the Remediation Engine component in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Real-Time Computer Protection** section.
4. In the **Remediation Engine** block, click the **Settings** button.
5. The **Remediation Engine** window opens on the **General** tab.
6. Do one of the following:
   - Select the **Remediation Engine** check box if you want to enable the Remediation Engine component.
   - Clear the **Remediation Engine** check box if you want to disable the Remediation Engine component.
7. Click the **OK** button in the **Remediation Engine** window.
8. Click the **OK** button in the **Properties: <Policy name>** window.

How to enable or disable the Remediation Engine component in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Real-Time Computer Protection** section.
5. In the **Remediation Engine** block, click the **Configure** button.
6. The **Remediation Engine** window opens.

7. Do one of the following:

   - Select the **Remediation Engine** check box if you want to enable the Remediation Engine component.
   - Clear the **Remediation Engine** check box if you want to disable the Remediation Engine component.

8. Click the **OK** button in the **Remediation Engine** window.
9. Click the **Save** button in the **<Policy name>** window.

How to enable or disable the Remediation Engine component in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Real-Time Computer Protection** → **Remediation Engine** section.
2. Click the **Properties** link in the results pane.
   The **Remediation Engine** window opens on the **General** tab.
3. Do one of the following:

   - Select the **Remediation Engine** check box if you want to enable the Remediation Engine component.
   - Clear the **Remediation Engine** check box if you want to disable the Remediation Engine component.

4. Click the **OK** button in the **Remediation Engine** window.

Anti-Cryptor

The Anti-Cryptor component receives data on the actions of applications on your computer and provides this information to other protection components to improve their performance. The Anti-Cryptor component utilizes Behavior Stream Signatures (BSS) for applications. If application activity matches a behavior stream signature, Kaspersky Industrial CyberSecurity for Nodes performs the selected responsive action. Kaspersky Industrial CyberSecurity for Nodes functionality based on behavior stream signatures provides proactive defense for the computer.

Enabling and disabling encryption protection for local folders

How to enable or disable Anti-Cryptor in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Use the **Anti-Cryptor** check box to enable or disable the component.
6. Go to the **General** tab.
7. Use the **Enable protection of local folders against external encryption** check box to enable or disable the option. If this check box is selected, Kaspersky Industrial CyberSecurity for Nodes responds to malicious activity with the action specified below.
8. Select the relevant action in the **Action on malware activity detection** block:
   - **Delete**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes deletes the executable file of the malicious application and creates a backup copy of the file in Backup.
   - **Block**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes terminates this application.
   - **Inform**. If this item is selected and malware activity of an application is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about the malware activity of the application to the list of active threats.
9. Save your changes. To apply the policy on computers, close the padlocks .

How to enable or disable Anti-Cryptor in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.

   The **Anti-Cryptor** window opens.

5. Use the **Enable Anti-Cryptor** check box to enable or disable the component.

6. Go to the **General** tab.

7. Use the **Enable protection of local folders against external encryption** check box to enable or disable the option. If this check box is selected, Kaspersky Industrial CyberSecurity for Nodes responds to malicious activity with the action specified below.

8. Select the relevant action in the **Upon detection of external encryption of shared folders** block:

   - **Delete**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes deletes the executable file of the malicious application and creates a backup copy of the file in Backup.

   - **Block**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes terminates this application.

   - **Inform**. If this item is selected and malware activity of an application is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about the malware activity of the application to the list of active threats.

9. Save your changes. To apply the policy on computers, close the padlocks .

How to enable or disable Anti-Cryptor in the Application Console

1. Select **Real-Time Computer Protection** → **Anti-Cryptor** in the Kaspersky Industrial CyberSecurity for Nodes Console tree.

2. Click **Properties** in the results pane of the **Anti-Cryptor** node.

   The **Properties: Anti-Cryptor** window opens.

3. Select the **Anti-Cryptor** check box.

4. Go to the **General** tab.

5. Use the **Enable protection of local folders against external encryption** check box to enable or disable the option. If this check box is selected, Kaspersky Industrial CyberSecurity for Nodes responds to malicious activity with the action specified below.

6. Select the relevant action in the **Upon detection of external encryption of shared folders** block:

   - **Delete**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes deletes the executable file of the malicious application and creates a backup copy of the file in Backup.

   - **Block**. If this item is selected, on detecting malicious activity Kaspersky Industrial CyberSecurity for Nodes terminates this application.

   - **Inform**. If this item is selected and malware activity of an application is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about the malware activity of the application to the list of active threats.

7. Save your changes.

Protection of shared folders against external encryption

The component monitors operations performed only with those files that are stored on mass storage devices with the NTFS file system and that are not encrypted with EFS.

Protection of shared folders against external encryption provides for the analysis of activity in shared folders. If this activity matches a behavior stream signature that is typical for external encryption, Kaspersky Industrial CyberSecurity for Nodes performs the selected action.

If an attempt to modify files in shared folders is detected, Kaspersky Industrial CyberSecurity for Nodes performs the following actions:

- Blocks access to file modification for the session that initiated the malicious activity (the file will be read-only).
- Creates backup copies of files that are being modified.
- Adds an entry to local application interface reports and sends information about the detected malicious activity to Kaspersky Security Center.
- Also, if the Remediation Engine component is enabled, the modified files are restored from backup copies.

Enabling and disabling protection of shared folders against external encryption

By default, protection of shared folders against external encryption is enabled and working as recommended by Kaspersky experts. To configure this functionality, you can create a protection scope and configure exclusions, if necessary. By default, the application automatically identifies shared folders and monitors file activity in all folders. If an attempt at external encryption of files in shared folders is detected, Kaspersky Industrial CyberSecurity for Nodes blocks the session of the remote user for one hour (by default).

After Kaspersky Industrial CyberSecurity for Nodes is installed, the protection of shared folders against external encryption will be limited until the computer is restarted.

How to enable or disable the protection of shared folders against external encryption in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Use the **Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.

7. Use the **Protect shared folders** check box to enable or disable the option.

8. Select the relevant action in the **Protection of shared folders against external encryption** block:

   - **Block connection for N min**. If this option is selected, when Kaspersky Industrial CyberSecurity for Nodes detects an attempt to modify files in shared folders, it blocks access to file modification (read only) for the session that initiated the malicious activity and creates backup copies of the modified files.

     If the Remediation Engine component is enabled and the **Block connection for N min** option is selected, modified files are restored from backup copies.

   - **Inform**. If this option is selected, then if an attempt to modify files in shared folders is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about this file modification attempt in shared folders to the list of active threats, adds a record to reports of the local interface of the application, and sends information about malicious activity detection to Kaspersky Security Center.

9. If necessary, create a protection scope and configure exclusions.

10. Save your changes. To apply the policy on computers, close the padlocks .

How to enable or disable the protection of shared folders against external encryption in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.

   The **Anti-Cryptor** window opens.

5. Use the **Enable Anti-Cryptor** check box to enable or disable the component.

6. Go to the **Protection of shared folders** tab.

7. Use the **Enable protection of shared folders against external encryption** check box to enable or disable the option.

8. Select the relevant action in the **Detection of external encryption** block:

   - **Block connection**. If this option is selected, when Kaspersky Industrial CyberSecurity for Nodes detects an attempt to modify files in shared folders, it blocks access to file modification (read only) for the session that initiated the malicious activity and creates backup copies of the modified files.

     If the Remediation Engine component is enabled and the **Block connection** option is selected, modified files are restored from backup copies.

   - **Inform**. If this option is selected, then if an attempt to modify files in shared folders is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about this file modification attempt in shared folders to the list of active threats, adds a record to reports of the local interface of the application, and sends information about malicious activity detection to Kaspersky Security Center.

9. If necessary, create a protection scope and configure exclusions.

10. Save your changes. To apply the policy on computers, close the padlocks.

How to enable or disable the protection of shared folders against external encryption in the Application Console

1. Select **Real-Time Computer Protection** → **Anti-Cryptor** in the Kaspersky Industrial CyberSecurity for Nodes Console tree.

2. Click **Properties** in the results pane of the **Anti-Cryptor** node.

   The **Properties: Anti-Cryptor** window opens.

3. Select the **Anti-Cryptor** check box.

4. Go to the **Protection of shared folders** tab.

5. Use the **Protect shared folders** check box to enable or disable the option.

6. Select the relevant action in the **Protection of shared folders against external encryption** block:

   - **Block connection for N min**. If this option is selected, when Kaspersky Industrial CyberSecurity for Nodes detects an attempt to modify files in shared folders, it blocks access to file modification (read only) for the session that initiated the malicious activity and creates backup copies of the modified files.

     If the Remediation Engine component is enabled and the **Block connection for N min** option is selected, modified files are restored from backup copies.

   - **Inform**. If this option is selected, then if an attempt to modify files in shared folders is detected, Kaspersky Industrial CyberSecurity for Nodes adds information about this file modification attempt in shared folders to the list of active threats, adds a record to reports of the local interface of the application, and sends information about malicious activity detection to Kaspersky Security Center.

7. If necessary, create a protection scope and configure exclusions.

8. Save your changes.

Editing the protection scope

A *protection scope* is a list of paths to shared folders in which Kaspersky Industrial CyberSecurity for Nodes monitors file activity. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: By default, the application automatically identifies shared folders and monitors file activity in all folders.

Excluding a folder from the protection scope can reduce the amount of false positives if your organization uses data encryption when exchanging files using shared folders. For example, the Anti-Cryptor component can raise false positives when the user works with files with the ENC extension in a shared folder. Such activity matches a behavioral pattern that is typical for external encryption. If you have encrypted files in a shared folder to protect data, add that folder to exclusions.

You can also exclude computers if you want attempts of external encryption coming from them to be ignored.

How to configure the protection scope in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Use the **Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. In the **Protection scope** block, click the **Configure** button.
8. In the window that opens, select the **Only specified shared folders** mode.
9. Click **Add**.
10. This opens a window; in that window, enter the path to the shared folder that you want to include in the protection scope (for example, `C:\Share`).

    To add a shared folder to the protection scope, use a local path.

11. Click **OK**.
12. If necessary, define protection scope exclusions:

    a. In the **Exclusions** block, click the **Configure** button.

    b. In the window that opens, click the **Add** button.

    c. In the displayed window, enter the path to the folder or file.

    Use masks:

    - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
    - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.
    - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

You can exclude an object from scans without removing it from the list of objects in the protection scope. To do so, clear the check box next to the object.

13. Save your changes. To apply the policy on computers, close the padlocks .

How to configure the protection scope in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.

   The **Anti-Cryptor** window opens.
5. Use the **Enable Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. Under **Protection scope**, select the **Only specified shared folders** mode.
8. Click **Add**.
9. This opens a window; in that window, enter the path to the shared folder that you want to include in the protection scope (for example, `C:\Share`).

   > To add a shared folder to the protection scope, use a local path.

10. Click **OK**.
11. If necessary, define protection scope exclusions:

    a. In the **Object to exclude** block, click the **Add** button.

    b. In the displayed window, enter the path to the folder or file.

Use masks:

- The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

- Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.

- The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

You can exclude an object from scans without removing it from the list of objects in the protection scope. To do so, clear the check box next to the object.

12. Save your changes. To apply the policy on computers, close the padlocks.

How to configure the protection scope in the Application Console

1. In the policy properties window, select **Real-Time Computer Protection**.
2. Click **Settings** in the **Anti-Cryptor** section.
3. Select **Real-Time Computer Protection** → **Anti-Cryptor** in the Kaspersky Industrial CyberSecurity for Nodes Console tree.
4. Click **Properties** in the results pane of the **Anti-Cryptor** node.

   The **Properties: Anti-Cryptor** window opens.
5. Use the **Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. In the **Protection scope** block, click the **Configure** button.
8. In the window that opens, select the **Only specified shared folders** mode.
9. In the **Protection scope** block, click the **Add** button.
10. This opens a window; in that window, enter the path to the shared folder that you want to include in the protection scope (for example, `C:\Share`).

    To add a shared folder to the protection scope, use a local path.

11. Click **OK**.

12. If necessary, define protection scope exclusions:

    a. In the **Exclusions** block, click the **Settings** button.

    b. In the displayed **Exclusions by mask** window, click the **Add** button.

    c. In the displayed window, enter the path to the folder or file.

    Use masks:

    - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

    - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask.

    - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

    You can exclude an object from scans without removing it from the list of objects in the protection scope. To do so, clear the check box next to the object.

13. Save your changes.

Adding trusted computers for external data encryption

If your organization uses external data encryption in its file exchange workflow, you must create a list of trusted computers. Kaspersky Industrial CyberSecurity for Nodes does not monitor data encryption from trusted computers.

On protected devices running Windows XP or Windows Server 2003, Kaspersky Industrial CyberSecurity for Nodes will monitor attempts to encrypt shared folders, even if you add a remote computer to the list of trusted computers.

The Audit Logon service must be enabled to enable exclusions of addresses from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

The functionality for excluding addresses from shared folder protection does not work on a remote computer if the remote computer was turned on before Kaspersky Industrial CyberSecurity for Nodes was started. You can restart this remote computer after Kaspersky Industrial CyberSecurity for Nodes is started to ensure that the functionality for excluding addresses from shared folder protection works on this remote computer.

How to add a trusted computer for external encryption of data in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Go to the **Protection of shared folders** tab.
6. In the **IP address exclusions** block, click the **Configure** button.
7. In the window that opens, click the **Add** button.
8. Enter the IP address or name of the computer from which external encryption attempts must not be handled.
9. Save your changes. To apply the policy on computers, close the padlocks .

How to add a trusted computer for external encryption of data in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.
   The **Anti-Cryptor** window opens.
5. Go to the **Protection of shared folders** tab.
6. In the **Exclusions** block, click the **Add** button.
7. Enter the IP address or name of the computer from which external encryption attempts must not be handled.
8. Save your changes. To apply the policy on computers, close the padlocks .

How to add a trusted computer for external encryption of data in the Application Console

1. Select **Real-Time Computer Protection** → **Anti-Cryptor** in the Kaspersky Industrial CyberSecurity for Nodes Console tree.
2. Click **Properties** in the results pane of the **Anti-Cryptor** node.
   The **Properties: Anti-Cryptor** window opens.
3. Go to the **Protection of shared folders** tab.
4. In the **IP address exclusions** block, click the **Configure** button.
5. In the window that opens, click the **Add** button.

6. Enter the IP address or name of the computer from which external encryption attempts must not be handled.
7. Save your changes.

Configuring the blocking period of an untrusted computer

An *untrusted computer* is a remote computer that is engaging in malicious activity or data encryption. By default, Kaspersky Industrial CyberSecurity for Nodes blocks a remote user's session for one hour. When the blocking period expires, Kaspersky Industrial CyberSecurity for Nodes removes the computer from the block list and restores access to the shared folder.

How to configure the blocking period of an untrusted computer in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Use the **Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. Under **Upon detection of external encryption of shared folders**, configure the blocking period of an untrusted computer that is engaging in malicious activity or data encryption.
8. Save your changes. To apply the policy on computers, close the padlocks .

How to configure the blocking period of an untrusted computer in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.

   The **Anti-Cryptor** window opens.
5. Use the **Enable Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. Under **Detection of external encryption**, configure the blocking period of an untrusted computer that is engaging in malicious activity or data encryption.
8. Save your changes. To apply the policy on computers, close the padlocks .

How to configure the blocking period of an untrusted computer in the Application Console

1. Select **Real-Time Computer Protection** → **Anti-Cryptor** in the Kaspersky Industrial CyberSecurity for Nodes Console tree.
2. Click **Properties** in the results pane of the **Anti-Cryptor** node.

   The **Properties: Anti-Cryptor** window opens.
3. Select the **Anti-Cryptor** check box.
4. Go to the **Protection of shared folders** tab.
5. Under **Protection of shared folders against external encryption**, configure the blocking period of an untrusted computer that is engaging in malicious activity or data encryption.
6. Save your changes.

Exporting and importing a list of exclusions from protection of shared folders against external encryption

You can export the list of exclusions to an XML file. Then you can modify the file to, for example, add a large number of addresses of the same type. You can also use the export/import function to back up the list of exclusions or to migrate the list to a different server.

How to export and import a list of exclusions in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Real-Time Computer Protection**.
4. Click **Settings** in the **Anti-Cryptor** section.
5. Go to the **Protection of shared folders** tab.
6. In the **IP address exclusions** block, click the **Configure** button.
7. To export the list of rules:

   a. If necessary, select the exclusions that you want to export.

   b. Click the button and select the export mode: export the whole list of exclusions or only selected exclusions.

   c. In the window that opens, specify the name of the XML file to which you want to export the list of exclusions, and select the folder in which you want to save this file.

   d. Save the file.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of exclusions to the XML file.

8. To import the list of exclusions:

    a. Click the → **Import** button.

    In the window that opens, select the XML file from which you want to import the list of exclusions.

    b. Open the file.

    Kaspersky Industrial CyberSecurity for Nodes imports the exclusions.

9. Save your changes. To apply the policy on computers, close the padlocks.

How to export and import a list of exclusions in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

    The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.

    The **Anti-Cryptor** window opens.
5. Use the **Enable Anti-Cryptor** check box to enable or disable the component.
6. Go to the **Protection of shared folders** tab.
7. To export the list of exclusions in the **Exclusions** block:

    a. If necessary, select the exclusions that you want to export.

    b. Click the **Export** button and select the export mode: export the whole list of exclusions or only selected exclusions.

    c. Save the file.

    Kaspersky Industrial CyberSecurity for Nodes exports the list of exclusions to the XML file.

8. To import the list of exclusions in the **Exclusions** block:

    a. Click the **Import** button and select an import mode: add or replace.

    b. In the window that opens, select the XML file from which you want to import the list of exclusions.

    c. Open the file.

    Kaspersky Industrial CyberSecurity for Nodes imports exclusions according to the selected mode.

9. Save your changes. To apply the policy on computers, close the padlocks.

Network Threat Protection

The Network Threat Protection component scans inbound network traffic for activity that is typical of network attacks. Upon detecting an attempted network attack that targets your computer, Kaspersky Industrial CyberSecurity for Nodes blocks network activity from the attacking computer. Descriptions of currently known types of network attacks and ways to counteract them are provided in the application databases. The list of network attacks that the Network Threat Protection component detects is updated during database and application module updates.

By default, the Network Threat Protection task runs in the **Inform** mode. In this mode, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, and logs event corresponding to the detected activity, but does not block the connection to the computers that are involved in such activity, and does not add the IP addresses of such computers to the list of blocked network sessions.

In the **Block** mode, Kaspersky Industrial CyberSecurity for Nodes blocks connection to computers that display activity typical of network attacks, and in some cases adds IP addresses of such computers to the list of blocked network sessions.

You can view the list of blocked hosts in the Blocked Hosts storage.

Kaspersky Industrial CyberSecurity for Nodes clears the block list when the application is restarted and when the Network Threat Protection settings are changed.

You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

The IP addresses of hosts showing activity typical of network attacks are deleted from the list of blocked hosts in the following cases:

- Kaspersky Industrial CyberSecurity for Nodes is uninstalled.
- The IP address was deleted manually from the list of blocked hosts.
- Host blocking term has expired.
- The **Block** mode was turned off.

For Kaspersky Industrial CyberSecurity for Nodes to work correctly on virtual machines in a Microsoft Hyper-V infrastructure, you need to install Kaspersky Industrial CyberSecurity for Nodes before you configure Hyper-V virtual switches.

Enabling and configuring Network Threat Protection

How to enable and configure Network Threat Protection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Network activity control** section.
4. In the **Network Threat Protection** block, click the **Settings** button.
5. In the window that opens, select the **Network Threat Protection** check box.
6. Select the task mode in the **Operating mode** section:
   - **Block**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, blocks connection to computers that display such activity, and in some cases adds IP addresses of computers to the list of blocked network sessions. The application also logs events about detected activity typical of network attacks in the component log.
   - **Inform**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, but does not block connection to computers that display such activity, and does not add IP addresses of computers to the list of blocked network sessions. The application logs events about detected activity typical of network attacks in the component log.
7. Use the **Treat port scanning and network flooding as attacks** check box to enable or disable the detection of the corresponding attacks.
8. If necessary, select the **Block attacking devices for N min** check box.
9. In the **MAC spoofing protection** block, select or clear the **Enable protection against MAC spoofing attacks** check box.
10. If necessary, you can add exclusions from blocking.
11. Save your changes.

How to enable and configure Network Threat Protection in the Application Console

1. In the Application Console tree, select the **Real-Time Computer Protection → Network Threat Protection** node.
2. Click the **Properties** link in the results pane.

   The **Properties: Network Threat Protection** window opens.
3. Select the **Network Threat Protection** check box.

4. Select the task mode in the **Operation mode** section:

   - **Block**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, blocks connection to computers that display such activity, and in some cases adds IP addresses of computers to the list of blocked network sessions. The application also logs events about detected activity typical of network attacks in the component log.

   - **Inform**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, but does not block connection to computers that display such activity, and does not add IP addresses of computers to the list of blocked network sessions. The application logs events about detected activity typical of network attacks in the component log.

5. Use the **Treat port scanning and network flooding as attacks** check box to enable or disable the detection of the corresponding attacks.

6. If necessary, select the **Block attacking devices for N min** check box.

7. In the **MAC spoofing protection** block, select or clear the **Enable protection against MAC spoofing attacks** check box.

8. If necessary, you can add exclusions from blocking.

9. Save your changes.

How to enable and configure Network Threat Protection in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select **Network activity control** → **Network Threat Protection**.

5. On the **General** tab, select the **Enable Network Threat Protection** check box.

6. Select the task operating mode:

   - **Block**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, blocks connection to computers that display such activity, and in some cases adds IP addresses of computers to the list of blocked network sessions. The application also logs events about detected activity typical of network attacks in the component log.

   - **Inform**. If this mode is selected, Kaspersky Industrial CyberSecurity for Nodes scans inbound network traffic for activity that is typical of network attacks, but does not block connection to computers that display such activity, and does not add IP addresses of computers to the list of blocked network sessions. The application logs events about detected activity typical of network attacks in the component log.

7. Use the **Treat port scanning and network flooding as attacks** check box to enable or disable the detection of the corresponding attacks.

8. If necessary, select the **Block attacking devices for N min** check box.

9. Select or clear the **Enable protection against MAC spoofing attacks** check box.

10. If necessary, you can add exclusions from blocking.

11. Save your changes.

Creating an exclusion from blocking

Kaspersky Industrial CyberSecurity for Nodes can recognize a network attack and block an unsecured network connection that is transmitting a large number of packets (for example, from surveillance cameras). To work with trusted devices, you can add the IP addresses of these devices to the list of exclusions. You can also select the protocol and port that are used for communication and allow specific network activities.

> The ability to select protocols and ports for exclusions was added in Kaspersky Industrial CyberSecurity for Nodes 4.0. Make sure the application and the management plug-in are updated to version 4.0 or later. If you are using an earlier version of the application or the management plug-in, Kaspersky Industrial CyberSecurity for Nodes can allow network activities only by IP address.

How to create an exclusion from blocking in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, go to the **Network activity control** section.

4. In the **Network Threat Protection** block, click the **Settings** button.
   The **Network Threat Protection** window opens.

5. Go to the **Exclusions** tab.

6. Select the **Do not control excluded addresses** check box to prevent Kaspersky Industrial CyberSecurity for Nodes from scanning inbound network traffic for excluded IP addresses.

7. Click **Add**.

8. In the **Exclusion** window, enter the IP address of the device network attacks from which will not be blocked.

9. If required, select the protocol and specify ports through which data is transmitted.

10. Click **OK**.

11. Perform steps c-f for every added exclusion.

12. Save your changes.

How to create an exclusion from blocking in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.

3. Select the **Application settings** tab.
4. Select **Network activity control** → **Network Threat Protection** and click the **Configure** button.
5. Go to the **Exclusions** tab.
6. Select the **Do not control excluded IP addresses** check box to prevent Kaspersky Industrial CyberSecurity for Nodes from scanning inbound network traffic for excluded IP addresses.
7. Click **Add**.
8. In the **Add exclusion** window, enter the IP address of the device network attacks from which will not be blocked.
9. If required, select the protocol and specify ports through which data is transmitted.
10. Click **OK**.
11. Perform steps c-f for every added exclusion.
12. Save your changes.

How to create an exclusion from blocking in the Application Console

1. In the Application Console tree, select the **Real-Time Computer Protection** → **Network Threat Protection** node.
2. Click the **Properties** link in the results pane.

   The **Properties: Network Threat Protection** window opens.
3. Go to the **Exclusions** tab.
4. Select the **Do not control excluded addresses** check box to prevent Kaspersky Industrial CyberSecurity for Nodes from scanning inbound network traffic for excluded IP addresses.
5. Click **Add**.
6. In the **Exclusion** window, enter the IP address of the device network attacks from which will not be blocked.
7. If required, select the protocol and specify ports through which data is transmitted.
8. Click **OK**.
9. Perform steps c-f for every added exclusion.
10. Save your changes.

Exporting and importing a list of exclusions from protection of shared folders against external encryption

You can export the list of exclusions to an XML file. Then you can modify the file to, for example, add a large number of addresses of the same type. You can also use the export/import function to back up the list of exclusions or to migrate the list to a different server.

How to export and import a list of exclusions in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Network activity control** section.
4. In the **Network Threat Protection** block, click the **Settings** button.

   The **Network Threat Protection** window opens.
5. Go to the **Exclusions** tab.
6. To export the list of rules, perform one of the following actions:

   - Using check boxes, select the exclusions that you want to export. Click the arrow and in the drop-down list select **Export selected**.
   - To export the entire list of exclusions, click the arrow and in the drop-down list select **Export**.

     Kaspersky Industrial CyberSecurity for Nodes saves a file named networkExclusions.xml in the standard download folder.
7. To import the list of exclusions:

   a. Click the arrow and select **Import**.

   b. In the window that opens, select the XML file from which you want to import the list of exclusions.

   c. Open the file.

   If the computer already has a list of exclusions, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.
8. Save your changes.

How to export and import a list of exclusions in the Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection → Network Threat Protection** and click the **Configure** button.
5. In the window that opens, select the **Exclusions** tab.
6. To export the list of rules:

   a. If necessary, select the exclusions that you want to export.

   b. Click the **Export** button and select the export mode: export the whole list of exclusions or only selected exclusions.

c. Click **Export**.

Kaspersky Industrial CyberSecurity for Nodes saves a file named networkExclusions.xml in the standard download folder.

7. To import the list of exclusions:

a. Click the **Import** button and select an import mode: **Add to existing entries** or **Overwrite existing entries**.

b. In the window that opens, select the XML file from which you want to import the list of exclusions.

c. Open the file.

Kaspersky Industrial CyberSecurity for Nodes imports exclusions according to the selected mode.

8. Save your changes.

AMSI Scanner

When the AMSI Scanner task is running, Kaspersky Industrial CyberSecurity for Nodes controls the execution of scripts created using Microsoft Windows scripting technologies (Active Scripting) such as VBScript or JScript. The application can also process PowerShell scripts and scripts run in the Microsoft Office applications on operating systems with the Antimalware Scan Interface (AMSI) installed.

AMSI allows applications and services to integrate with any antimalware application installed on a device in order for all the executed scripts to be intercepted and scanned by the antimalware. You can find more information about AMSI functionality on the Microsoft website.

In component settings, you can allow or deny the running of dangerous scripts. If Kaspersky Industrial CyberSecurity for Nodes identifies a script as dangerous, it blocks or allows execution of the script according to your selected action. If you select the **Block** action, the application blocks dangerous scripts and allows other scripts.

Kaspersky Industrial CyberSecurity for Nodes supports the AMSI technology in Microsoft Windows 10 and Microsoft Windows Server 2016 and later.

Enabling and disabling AMSI Scanner

How to enable or disable AMSI Scanner in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Real-Time Computer Protection** section.
4. In the **AMSI Scanner** block, click the **Settings** button.
   The **AMSI Scanner** window opens on the **General** tab.
5. Do one of the following:
   - Select the **AMSI Scanner** check box if you want to enable the AMSI Scanner.
   - Clear the **AMSI Scanner** check box if you want to disable the AMSI Scanner.
6. Save your changes.

How to enable AMSI Scanner in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Real-Time Computer Protection** → **AMSI Scanner** section.
2. Click the **Properties** link in the results pane.
   The **AMSI Scanner** window opens on the **General** tab.

3. Do one of the following:

   - Select the **AMSI Scanner** check box if you want to enable the AMSI Scanner.
   - Clear the **AMSI Scanner** check box if you want to disable the AMSI Scanner.

4. In the **AMSI Scanner** window, click the **OK** button.

How to enable AMSI Scanner in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Real-Time Computer Protection** section.
5. In the **AMSI Scanner** block, click the **Configure** button.
   The **AMSI Scanner** window opens.
6. Do one of the following:

   - Select the **AMSI Scanner** check box if you want to enable the AMSI Scanner.
   - Clear the **AMSI Scanner** check box if you want to disable the AMSI Scanner.

7. Save your changes.

AMSI Scanner settings

How to configure AMSI Scanner settings in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Real-Time Computer Protection** section.
4. In the **AMSI Scanner** block, click the **Settings** button.
   The **AMSI Scanner** window opens on the **General** tab.
5. Select the action that you want Kaspersky Industrial CyberSecurity for Nodes to perform when a dangerous script is run:

   - **Inform**. The application allows running probably dangerous scripts. A corresponding event is logged in the task log.
   - **Block**. The application blocks probably dangerous scripts.

6. In the **Scan of compound files** block, specify the types of compound files that you want to scan: archives, distribution package, or files in office formats.

7. In the **Size limit** block, do one of the following:

   - To block the AMSI Scanner component from unpacking large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size (MB)** field. The AMSI Scanner component will not unpack compound files that are larger than the specified size.

   - To allow the AMSI Scanner component to unpack large compound files, clear the **Do not unpack large compound files** check box.

   The AMSI Scanner component scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

8. In the **AMSI Scanner** window, click the **OK** button.

9. Click the **OK** button in the **Properties: <Policy name>** window.

How to configure AMSI Scanner settings in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Real-Time Computer Protection** → **AMSI Scanner** section.

2. Click the **Properties** link in the results pane.

   The **AMSI Scanner** window opens on the **General** tab.

3. Select the action that you want Kaspersky Industrial CyberSecurity for Nodes to perform when a dangerous script is run:

   - **Inform**. The application allows running probably dangerous scripts. A corresponding event is logged in the task log.

   - **Block**. The application blocks probably dangerous scripts.

4. In the **Scan of compound files** block, specify the types of compound files that you want to scan: archives, distribution package, or files in office formats.

5. In the **Size limit** block, do one of the following:

   - To block the AMSI Scanner component from unpacking large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size (MB)** field. The AMSI Scanner component will not unpack compound files that are larger than the specified size.

   - To allow the AMSI Scanner component to unpack large compound files, clear the **Do not unpack large compound files** check box.

   The AMSI Scanner component scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

6. In the **AMSI Scanner** window, click the **OK** button.

How to configure AMSI Scanner settings in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Real-Time Computer Protection** section.
5. In the **AMSI Scanner** block, click the **Configure** button.

   The **AMSI Scanner** window opens.
6. Select the action that you want Kaspersky Industrial CyberSecurity for Nodes to perform when a dangerous script is run:

   - **Inform**. The application allows running probably dangerous scripts. A corresponding event is logged in the task log.
   - **Block**. The application blocks probably dangerous scripts.
7. In the **Scan of compound files** block, specify the types of compound files that you want to scan: archives, distribution package, or files in office formats.
8. In the **Size limit** block, do one of the following:

   - To block the AMSI Scanner component from unpacking large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size (MB)** field. The AMSI Scanner component will not unpack compound files that are larger than the specified size.
   - To allow the AMSI Scanner component to unpack large compound files, clear the **Do not unpack large compound files** check box.

   The AMSI Scanner component scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.
9. Click the **OK** button in the **AMSI Scanner** window.
10. Click the **Save** button in the **<Policy name>** window.

Applications Launch Control

The Applications Launch Control component of Kaspersky Industrial CyberSecurity for Nodes protects devices from unauthorized application launches. Applications Launch Control relies on the Default Deny principle, which means that any applications that are not allowed in the component settings will be blocked automatically. You can allow launching applications by creating component allowing rules for them.

If the Applications Launch Control rules are created to the fullest extent possible, Kaspersky Industrial CyberSecurity for Nodes blocks the launch of all new applications that are not verified by the administrator of the organization's local network, but ensures the performance of the operating system and verified applications that users need to perform their job duties. You can receive information about applications installed on protected devices using the *Rule Generator for Applications Launch Control* task.

If the Applications Launch Control component is enabled, Kaspersky Industrial CyberSecurity for Nodes intercepts every operating system event related to a request to create a process that occurs when an executable file is launched on a protected device. The application then collects information about the executable file, script, or MSI package being launched and compares it with the conditions for triggering the Applications Launch Control rules. If all conditions of at least one allowing rule are met, Kaspersky Industrial CyberSecurity for Nodes allows the startup of the application. If the application being launched does not meet the conditions of any allowing rule, or if a blocking rule is triggered, Kaspersky Industrial CyberSecurity for Nodes blocks the attempt to start the application by canceling the process creation.

All attempts to start applications are recorded in the component's log.

The Applications Launch Control component can operate in one of two modes:

- **Block**. Kaspersky Industrial CyberSecurity for Nodes controls the launch of applications using Applications Launch Control rules. The scope of Applications Launch Control rules is specified in the general settings of the Applications Launch Control component. If an application satisfies Applications Launch Control rules, but none of the rules matches the scope of Applications Launch Control rules, such applications are prevented from running.

  Running applications that are not covered by Applications Launch Control rules is prohibited.

  The Applications Launch Control component cannot be started in Active mode if no Applications Launch Control rules have been created or if more than 65,535 Applications Launch Control rules exist for one protected device.

- **Inform**. Kaspersky Industrial CyberSecurity for Nodes allows the startup of all applications. Only information is recorded about all application launches, rules that cover the launched applications, and actions that would be performed if the task was running in **Block** mode. This mode is set by default.

When creating Applications Launch Control rules, we recommend making sure that they do not block your operating system's applications from running.

Kaspersky Industrial CyberSecurity for Nodes also intercepts processes launched under the Windows Subsystem for Linux (except for scripts run from the UNIX™ shell, or command line interpreters). For such processes, the Applications Launch Control component applies the actions defined by the current configuration. The *Rule Generator for Applications Launch Control* task detects application launches and generates corresponding rules for applications running under the Windows Subsystem for Linux.

About Applications Launch Control rules

How Applications Launch Control rules work

The operation of Applications Launch Control rules is based on the following components:

- Type of rule.

  Applications Launch Control rules can allow or deny the start of applications. Accordingly, they are called *allowing* or *denying* rules.

- Rule usage scope.

  Applications Launch Control rules can be applied to *executable files*, *scripts*, and *MSI packages*.

- Rule-triggering conditions.

  Applications Launch Control rules regulate the launch of files that satisfy at least one trigger conditions specified in the rule settings. For example, executable files are signed with the specified *digital certificate*, have the specified *SHA256 hash*, are located at the specified *path*, match the specified *command line* arguments. You must add at least one rule triggering condition. Otherwise, the Application Launch Control rule is not added.

- Exclusions from the rule.

  You can configure exclusions for the Applications Launch Control rule, which may be based on the same criteria as the rule triggering conditions. Exclusions to Applications Launch Control rules may be required for certain allowing rules: for example, if you want to allow users to start applications from the C:\Windows path, while blocking launch of the Regedit.exe file.

- User or group of users.

  Applications Launch Control rules can control the start of specified applications by specified users and / or user groups.

When creating Applications Launch Control rules, we recommend making sure that the new rules do not block your operating system's applications from running.

Managing Applications Launch Control rules

You can perform the following actions with Applications Launch Control rules:

- Add manually.
- Generate and add rules automatically.
- Delete.

- Import and export.
- Filter the list of rules.

About Software Distribution Control

Generating Applications Launch Control may become more complicated if you want to control the distribution of software. For example, you may want to do it on protected devices where installed software are automatically updated on a regular basis. In this case, the list of allowing rules must be updated after each software update for newly created files to be considered in the Applications Launch Control component settings. To simplify launch control in software distribution scenarios, you can use Software Distribution Control.

An *installation package* (hereinafter referred to as package) represents one or several applications to be installed on a protected device. An installation package may also contain updates and individual commands.

The Software Distribution Control subsystem is implemented as an additional list of exclusions. When an installation package is added to the list, it becomes trusted. Unpacking is allowed for trusted packages, and automatic startup is allowed for applications installed or updated from trusted packages. The extracted files can inherit the trusted attribute of the primary distribution package. A *primary distribution package* is a package that has been added to the list of Software Distribution Control exclusions by a user and has become a trusted package.

Kaspersky Industrial CyberSecurity for Nodes controls only the full cycle of application distribution and cannot correctly process the launch of files modified by a trusted package if, when the package is started for the first time, Software Distribution Control is turned off or the Applications Launch Control component is not installed.

To use Software Distribution Control, you must enable the **Apply rules to executable files** functionality in the Applications Launch Control component general settings.

Software distribution cache

Kaspersky Industrial CyberSecurity for Nodes uses a dynamically generated software distribution cache (hereinafter referred to as distribution cache) to establishes the relationship between trusted packages and files created during software distribution. When a package is first started, Kaspersky Industrial CyberSecurity for Nodes detects all files created by the package during the software distribution process and stores file checksums and paths in the distribution cache. Then, by default, all files that have information saved in the distribution cache are allowed to start.

You cannot review, delete, or manually modify the distribution cache via the user interface. The cache is populated and controlled by Kaspersky Industrial CyberSecurity for Nodes.

You can export the distribution cache to a configuration file (XML format) or delete the distribution cache on the command line.

Kaspersky Industrial CyberSecurity for Nodes updates the distribution cache every 24 hours. If the checksum of a previously allowed file is changed, the application deletes the record for this file from the distribution cache. If the Applications Launch Control component is running in Active mode, subsequent attempts to start this file will be blocked. If the full path to the previously allowed file is changed, subsequent attempts to start this file will not be blocked, because the checksum is stored within the distribution cache.

Processing the extracted files

Extracted files and packages created by a primary trusted distribution package (at the first level of nesting) inherit the trusted attribute when their checksums are added to the distribution cache when the software distribution package in the exclusion list is opened for the first time. Hence, the distribution package itself and all files extracted from this package will also be trusted.

For example, if test.msi, a package containing several packages and applications, is added to the list of exclusions and the **Allow launching of all child files as trusted distribution packages** functionality is enabled, all packages and applications contained in the test.msi package can be unpacked and run, even if they contain other nested files. This scenario works for extracted files on all nested levels.

If the test.msi package is added to the list of exclusions, and the **Allow launching of all child files as trusted distribution packages** functionality is disabled, the application assigns the trusted attribute only to those packets and executable files that have been extracted directly from the trusted packet (at the first level of nesting). The checksums of such files are stored in the distribution cache. All files on the second level of nesting and beyond will be blocked by the Default Deny principle.

Extracted files will retain the trusted attribute after the operating system restarts.

To remove the inheritance attribute from all extracted files, you must delete the distribution cache and disable the **Allow launching of all child files as trusted distribution packages** functionality before you run the trusted installation package again.

Working with the Applications Launch Control rule list

The list of trusted packages of Software Distribution Control is a list of exclusions, which amplifies, but does not replace the general list of applications launch control rules.

Denying applications launch control rules have the highest priority: trusted package decompression and start of new or modified files will be blocked, if these packages and files are affected by the applications launch control denying rules.

Software distribution control exclusions are applied both for trusted packages and files created or modified by these packages, if no denying rules in the applications launch control list are applied for those packages and files.

About the Rule Generator for Applications Launch Control

You can create lists of Applications Launch Control rules using Kaspersky Security Center tasks and policies simultaneously for all protected devices and groups of protected devices on the corporate network. The scenarios listed below are recommended if the corporate network does not have a reference machine and you are unable to create a list of allowing rules based on applications installed on the template machine.

You can run the *Rule Generator for Applications Launch Control* task locally via the Application Console to create a list of rules based on the applications running on a single protected device.

You can create lists of Applications Launch Control rules on the side of Kaspersky Security Center in one of the following ways:

- Using the *Rule Generator for Applications Launch Control* group task.

  The*Rule Generator for Applications Launch Control* task, depending on the settings, can collect information about applications running on protected devices, as well as executable files and scripts located in the specified scopes. Based on the collected information, the task generates a list of allow rules for the Applications Launch Control component.

  You can configure automatic import of generated rules to the list of Applications Launch Control component rules, or import the generated rules manually.

  This scenario is recommended when you need to quickly create lists of Applications Launch Control rules. We recommend that you configure the scheduled launch of the *Rule Generator for Applications Launch Control* task only if the allowing rules usage scope includes folders and files you know to be safe.

- Based on the event report generated in Kaspersky Security Center for the Applications Launch Control component, running in *Inform* mode.

  Under this scenario, Kaspersky Industrial CyberSecurity for Nodes does not deny the launch of applications. Instead, with the Applications Launch Control component running in the *Inform* mode, it reports all allowed and denied application launches across all network protected devices in the **Events** tab of the Administration Server node's workspace in the Kaspersky Security Center. Kaspersky Security Center uses the reports to generate a single list of events in which application launches were denied.

  While the component is running, all possible scenarios for protected devices and protected device groups must be executed, including at least one restart of a protected device. You can then import application launch data from the saved Kaspersky Security Center event report (TXT format) and generate Applications Launch Control allowing rules for such applications based on this data.

  This scenario is recommended if a corporate network includes a large number of protected devices of different type (with a different software installed).

- Based on denied application launch events received through Kaspersky Security Center, without creating and importing a configuration file.

  To use this feature, the Applications Launch Control component on the protected device must be running under an active Kaspersky Security Center policy. In this case, all events on the protected device are sent to the Administration Server.

We recommend that you update the list of rules when the set of applications installed on network protected devices changes (for example, when updates are installed or operating systems are reinstalled). We recommend that you generate an updated list of rules by running the *Rule Generator for Applications Launch Control* task or the Applications Launch Control component in the *Inform* mode on protected devices in the test administration group. The test administration group includes the protected devices required to test the launch of new applications before they are installed on network protected devices.

XML files containing lists of allowing rules are created based on an analysis of applications started on the protected device. To account for all applications used on the network when generating lists of rules you are advised to start the *Rule Generator for Applications Launch Control* task and the Applications Launch Control component in the *Inform* mode on a template machine.

Before generating allowing rules based on the applications launched on a reference machine, make sure that the template machine is secure and there is no malware on it.

Before adding allowing rules, select one of the available rule application modes. The list of Kaspersky Security Center policy rules displays only rules specified by the policy, regardless of the rule application mode. The local rule list includes all applied rules — both local rules and rules added through a policy.

Enabling and configuring Applications Launch Control

How to enable and configure general settings for Applications Launch Control in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **Applications Launch Control** block, click the **Settings** button.
   The **Applications Launch Control** window opens on the **General** tab.
5. Select the **Applications Launch Control** check box.
6. In the **Operating mode for blocking rules** block, select the component operating mode:
   - **Block**. Kaspersky Industrial CyberSecurity for Nodes applies all created Applications Launch Control rules.
   - **Inform**. Kaspersky Industrial CyberSecurity for Nodes does not use Applications Launch Control rules. It only records information about the start of applications in the component's log. All applications are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about denied application launches recorded in the component's log.
7. Configure component settings (see the table below).
8. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes immediately applies the new component settings. Information about the date and time when the settings were modified, and the values of the settings before and after modification, are saved in the system audit log.

How to enable and configure general settings for Applications Launch Control in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.
2. Click the **Properties** link in the results pane.

   The **Applications Launch Control** window opens on the **General** tab.
3. Select the **Applications Launch Control** check box.
4. In the **Operating mode for blocking rules** block, select the component operating mode:

   - **Block**. Kaspersky Industrial CyberSecurity for Nodes applies all created Applications Launch Control rules.
   - **Inform**. Kaspersky Industrial CyberSecurity for Nodes does not use Applications Launch Control rules. It only records information about the start of applications in the component's log. All applications are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about denied application launches recorded in the component's log.
5. Configure component settings (see the table below).
6. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes immediately applies the new component settings. Information about the date and time when the settings were modified, and the values of the settings before and after modification, are saved in the system audit log.

How to enable and configure general settings for Applications Launch Control in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Local activity control** section.
5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.
6. Select the **Enable Applications Launch Control** check box.
7. In the **Operating mode for blocking rules** block, select the component operating mode:

   - **Block**. Kaspersky Industrial CyberSecurity for Nodes applies all created Applications Launch Control rules.
   - **Inform**. Kaspersky Industrial CyberSecurity for Nodes does not use Applications Launch Control rules. It only records information about the start of applications in the component's log. All applications are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about denied application launches recorded in the component's log.

8. Configure component settings (see the table below).

9. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes immediately applies the new component settings. Information about the date and time when the settings were modified, and the values of the settings before and after modification, are saved in the system audit log.

Applications Launch Control general settings

Parameter	Description
Repeat action taken for the first file launch on all the subsequent launches for this file	The option enables or disables launch control for the second and subsequent attempts to start applications based on the event information stored in the cache. If the option is enabled, Kaspersky Industrial CyberSecurity for Nodes allows or denies subsequent launches of an application based on the component's conclusion regarding the first launch of the application. For example, if the first application launch was allowed by the rules, information about this decision will be stored in the cache, and the second and all subsequent launches will also be allowed without rechecking. If the application is installed on a computer running Windows XP, when working with files through Explorer, the first application startup conclusions may be overwritten, causing the function to not work properly. If the option is disabled, Kaspersky Industrial CyberSecurity for Nodes analyzes an application every time a launch is attempted.
Deny the command interpreters launch with no command to execute	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes denies launching of a command-line interpreter when any of the following conditions is met: • The launch of a command-line interpreter is denied by Applications Launch Control rules. • The command-line interpreter starts without parameters. If the option is disabled, Kaspersky Industrial CyberSecurity for Nodes only considers allowing rules when launching a command line interpreter. Launch is blocked if none of the Applications Launch Control allow rules is applicable. If the allowing rule of Applications Launch Control applies, a command line interpreter can be launched with or without a command to execute. Kaspersky Industrial CyberSecurity for Nodes controls the launch of the following command interpreters: • cmd.exe • powershell.exe • python.exe • perl.exe • wscript.exe By default, the functionality is disabled.
Apply rules to executable files	The option either enables or disables launch control of executable files. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows or denies the launch of executable files using Applications Launch Control rules. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes does not control the launch of executable files using Applications Launch Control rules. Startup of executable files is allowed. This option is enabled by default.
Monitor loading of DLL modules	Controlling loading of DLL modules may affect the performance of the operating system. This functionality is available if the **Apply rules to executable files** functionality is enabled. This functionality enables or disables the control of loading of DLL modules. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows or denies the loading of DLL modules using Applications Launch Control rules. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes does not control the loading of DLL modules using Applications Launch Control rules. Loading of DLL modules is allowed. By default, the functionality is disabled.
Apply rules to scripts and MSI packages	The option either enables or disables launch of scripts and MSI packages. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows or denies the launch of scripts and MSI packages using Applications Launch Control rules. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes does not control the launch of MSI scripts and packages using Applications Launch Control rules. Start of scripts and MSI packages is allowed. This option is enabled by default.

Parameter	Description
Ignore a missing signature timestamp when validating certificates	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows launching applications that are signed with certificates that have expired or have an undefined expiration date. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes denies launching applications that are signed with certificates that have expired or have an undefined expiration date. By default, the functionality is disabled.

Configuring Software Distribution Control

How to configure Software Distribution Control in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **Applications Launch Control** block, click the **Settings** button.

   The **Applications Launch Control** window opens on the **General** tab.
5. Select the **Software Distribution Control** tab.
6. Enable the **Automatically allow software distribution via applications and packages listed** functionality. This functionality automatically creates exclusions for all files launched using executable files and installation packages specified in the list.

   You can enable the **Automatically allow software distribution via applications and packages listed** functionality if on the **General** tab, the **Apply rules to executable files** functionality is enabled.
7. If necessary, disable the **Always allow software distribution via Windows Installer** functionality. This functionality automatically creates exclusions for all files launched using the Windows installer.

   Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.
8. If necessary, enable the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** functionality. This functionality allows distributing software using the System Center Configuration Manager solution.

   If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows Microsoft Windows deployment using the System Center Configuration Manager. The application allows software distribution only via the Background Intelligent Transfer Service. The application controls the launch of executable files with .EXE and .MSI extensions.

   The application controls the software distribution cycle on the protected device — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of Kaspersky Industrial CyberSecurity for Nodes on the protected device.

9. Add executable files and installation packages that you want to allow to launch:

- **Add one manually**

  a. In the context menu of the **Add** button, select **Add one distribution package**.

  b. In the window that opens, click the **Browse** button.

  c. Select the executable file or distribution package.

  Fields under **Trusting criteria** are automatically populated with information about the selected file.

  d. If necessary, enable the **Allow launching of all child files as trusted distribution packages** functionality.

  e. Select the criterion that will decide that the executable file or installation package is trusted: **Certificate details** or **SHA256 hash**.

  f. Click **OK**.

  The executable file or installation package is added to the list.

- **Add several by hash**

  a. In the context menu of the **Add** button, select **Add several packages by hash**.

  b. This opens a window; in that window, select any number of files or installation packages.

  c. Click **Open**.

  Executable files or installation packages are added to the list. The SHA256 hash is specified in their properties.

- **Import from file**

  a. Click **Import**.

  b. In the window that opens, select a .TXT file with information about executable files and installation packages.

  c. Click **Open**.

  Executable files or installation packages are added to the list. The SHA256 hash is specified in their properties.

If you create a trusted distribution package based on an executable file and, providing you added a process in the Trusted Zone settings based on that same executable file and made it trusted for the Applications Launch Control component, the Trusted Zone settings have a higher priority. Kaspersky Industrial CyberSecurity for Nodes blocks this executable file from starting, but considers the executable file's process to be trusted.

10. If necessary, edit the list of added executable files and installation packages by clicking the **Edit** button.

11. If necessary, remove the added executable files and installation packages by clicking the **Delete** button. In this case, unpacked executable files are allowed to run.

    To prevent the execution of unpacked executable files, you must remove Kaspersky Industrial CyberSecurity for Nodes from the protected device or create Applications Launch Control deny rules for the unpacked files.

12. Click **OK**.

How to configure Software Distribution Control in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.
2. Click the **Properties** link in the results pane.

   The **Applications Launch Control** window opens on the **General** tab.
3. Select the **Software Distribution Control** tab.
4. Enable the **Automatically allow software distribution via applications and packages listed** functionality. This functionality automatically creates exclusions for all files launched using executable files and installation packages specified in the list.

   You can enable the **Automatically allow software distribution via applications and packages listed** functionality if on the **General** tab, the **Apply rules to executable files** functionality is enabled.
5. If necessary, disable the **Always allow software distribution via Windows Installer** functionality. This functionality automatically creates exclusions for all files launched using the Windows installer.

   Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.
6. If necessary, enable the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** functionality. This functionality allows distributing software using the System Center Configuration Manager solution.

   If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows Microsoft Windows deployment using the System Center Configuration Manager. The application allows software distribution only via the Background Intelligent Transfer Service. The application controls the launch of executable files with .EXE and .MSI extensions.

   The application controls the software distribution cycle on the protected device — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of Kaspersky Industrial CyberSecurity for Nodes on the protected device.
7. Add executable files and installation packages that you want to allow to launch:

   - **Add one manually**

     a. In the context menu of the **Add** button, select **Add one distribution package**.

     b. In the window that opens, click the **Browse** button.

c. Select the executable file or distribution package.

Fields under **Trusting criteria** are automatically populated with information about the selected file.

d. If necessary, enable the **Allow launching of all child files as trusted distribution packages** functionality.

e. Select the criterion that will decide that the executable file or installation package is trusted: **Certificate details** or **SHA256 hash**.

f. Click **OK**.

The executable file or installation package is added to the list.

- **Add several by hash**

a. In the context menu of the **Add** button, select **Add several packages by hash**.

b. This opens a window; in that window, select any number of files or installation packages.

c. Click **Open**.

Executable files or installation packages are added to the list. The SHA256 hash is specified in their properties.

- **Import from file**

a. Click **Import**.

b. In the window that opens, select a .TXT file with information about executable files and installation packages.

c. Click **Open**.

Executable files or installation packages are added to the list. The SHA256 hash is specified in their properties.

If you create a trusted distribution package based on an executable file and, providing you added a process in the Trusted Zone settings based on that same executable file and made it trusted for the Applications Launch Control component, the Trusted Zone settings have a higher priority. Kaspersky Industrial CyberSecurity for Nodes blocks this executable file from starting, but considers the executable file's process to be trusted.

8. If necessary, edit the list of added executable files and installation packages by clicking the **Edit** button.

9. If necessary, remove the added executable files and installation packages by clicking the **Delete** button. In this case, unpacked executable files are allowed to run.

To prevent the execution of unpacked executable files, you must remove Kaspersky Industrial CyberSecurity for Nodes from the protected device or create Applications Launch Control deny rules for the unpacked files.

10. Click **OK**.

How to configure Software Distribution Control in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Local activity control** section.
5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.
6. Select the **Software Distribution Control** tab.
7. Enable the **Automatically allow software distribution via applications and packages listed** functionality. This functionality automatically creates exclusions for all files launched using executable files and installation packages specified in the list.

   > You can enable the **Automatically allow software distribution via applications and packages listed** functionality if on the **General** tab, the **Apply rules to executable files** functionality is enabled.
8. If necessary, disable the **Always allow software distribution via Windows Installer** functionality. This functionality automatically creates exclusions for all files launched using the Windows installer.

   > Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.
9. If necessary, enable the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** functionality. This functionality allows distributing software using the System Center Configuration Manager solution.

   If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows Microsoft Windows deployment using the System Center Configuration Manager. The application allows software distribution only via the Background Intelligent Transfer Service. The application controls the launch of executable files with .EXE and .MSI extensions.

   > The application controls the software distribution cycle on the protected device — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of Kaspersky Industrial CyberSecurity for Nodes on the protected device.
10. Add executable files and installation packages that you want to allow to launch:

    - **Manually**

      a. Click the **Add** button.

      b. Under **Trusting criteria**, select the criterion that will decide that the executable file or installation package is trusted: **Use digital certificate** or **Use SHA256 hash**.

c. If you selected **Use digital certificate**, enter the header and thumbprint of the certificate that the executable file or installation package is signed with, and also the name of the executable file or installation package.

d. If you selected **Use SHA256 hash**, click **Browse** to select the executable file or installation package.

e. If necessary, enable the **Allow launching of all child files as trusted distribution packages** functionality.

f. Click **OK**.

The executable file or installation package is added to the list.

- **Import from file**

a. Click **Import**.

b. In the window that opens, select a .TXT file with information about executable files and installation packages.

c. Click the **Open** button.

Executable files or installation packages are added to the list. The SHA256 hash is specified in their properties.

If you create a trusted distribution package based on an executable file and, providing you added a process in the Trusted Zone settings based on that same executable file and made it trusted for the Applications Launch Control component, the Trusted Zone settings have a higher priority. Kaspersky Industrial CyberSecurity for Nodes blocks this executable file from starting, but considers the executable file's process to be trusted.

11. If necessary, edit the list of added executable files and installation packages by clicking the **Edit** button.
12. If necessary, remove the added executable files and installation packages by clicking the **Delete** button. In this case, unpacked executable files are allowed to run.

    To prevent the execution of unpacked executable files, you must remove Kaspersky Industrial CyberSecurity for Nodes from the protected device or create Applications Launch Control deny rules for the unpacked files.

13. Click **OK**.
14. Click the **OK** button in the **Applications Launch Control** window.

Working with Applications Launch Control rules

This section provides instructions for creating a list of rules for Applications Launch Control.

Adding Applications Launch Control rules

How to add Applications Launch Control rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **Applications Launch Control** block, click the **Settings** button.

   The **Applications Launch Control** window opens on the **General** tab.
5. Select the **Rules** tab.
6. In the **Rule usage** drop-down list, select the rule application mode:

   - **Add policy rules to the local rules**. The application applies the rule list specified in a policy together with local rule lists.
   - **Replace local rules with policy rules**. The application applies the rule list specified in the policy for application launch control on a group of protected devices. Local rule lists cannot be created, edited, or applied.
7. If necessary, enable the **Deny modification of local rules by users** functionality.

   If this functionality is enabled, the application does not allow editing Applications Launch Control rules locally in the Application Console. By default, the functionality is disabled.
8. Add Applications Launch Control rules in any of the following ways:

   - **Manually**

     a. Click **Add**.

     The **Applications Launch Control** window opens.

     b. In the **Name** field, enter the name of the rule.

     c. If necessary, in the **Description** field, enter a description of the rule.

     d. In the **Type** drop-down list, select the rule type:

     - **Allowing** if you want the rule to allow running applications described by the rule.
     - **Denying** if you want the rule to block the launch of applications described by the rule.

     e. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

     - **Executable files**, if you want the rule to control launch of executable files.
     - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages. Files with the following extensions are supported: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Select the **Trusted Updaters** check box if you want Kaspersky Industrial CyberSecurity for Nodes to consider applications matching the rule trigger conditions as trusted updaters. Trusted Updaters are applications that are allowed to create other executable files that will be allowed to run subsequently.

If an application triggers multiple rules, Kaspersky Industrial CyberSecurity for Nodes sets the *Trusted Updaters* flag if the following conditions are satisfied:

- All rules allow the application to run.
- At least one rule has the **Trusted Updaters** check box selected.

g. Add trigger conditions for the Applications Launch Control rule.

h. Add exclusions from trigger conditions for the Applications Launch Control rule.

i. Add users and/or groups of users that are allowed or forbidden to launch applications that satisfy the rule.

j. Click **OK**.

- **By importing an XML file containing Applications Launch Control rules**

a. In the context menu of the button, select the **Import → From XML file** item.

b. Choose how to add Device Control rules from an XML file to those available in the policy:

- **Replace existing rules**, if you want to replace the existing rules with the imported rules.
- **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
- **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

c. In the window that opens, specify the path to the XML file that was created after the completion of local task or group task for *Rule Generator for Applications Launch Control*.

d. Click **Open**.

- **Based on Kaspersky Security Center events using a request**

a. In the context menu of the button, select the **Import → Create allowing rules based on Kaspersky Security Center events (request)** item.

b. Select the principle for adding the rules to the list of previously created Application Launch Control rules:

- **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
- **Replace existing rules**, if you want to replace the existing rules with the imported rules.
- **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

The **Applications launch control rules generation** window opens.

c. Select the event types based on which the application will create Applications Launch Control rules:

- **Application launch denied**.
- **Statistics only mode: application launch denied**.

d. Select a period from the **Request events that were generated within the period** drop-down list.

e. Clear or select the **Prioritize the use of hash when generating rules** check box.

If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes uses the checksum of the file to generate the rule when both the checksum and the certificate of the file are available.

If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes uses the digital certificate of the file to generate the rule when both the checksum and the certificate of the file are available.

f. Click **Generate rules**.

g. Click **OK**.

- **By importing a TXT file with a selection of Kaspersky Security Center blocked application events**

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Logs and notifications** section.
4. In the **Task logs** block, click the **Settings** button.

The **Notifications** window opens.

5. Expand the **Local activity control** node.
6. Select the **Applications Launch Control** section.
7. In the list of Applications Launch Control events, in the **Send events to Kaspersky Security Center** column, select check boxes next to *Application startup prohibited* and *Application startup prohibited in test mode*.
8. Save your changes.
9. In the **Event configuration** section of the policy, make sure that the event storage duration specified in the **Store in the Administration Server database for (days)** field is greater than the period for which you plan to gather information about prevented application launches (the default is 30 days).

> Once the Applications Launch Control component log retention period expires, logged events will be deleted and will not appear in the report.

10. Activate the policy configured to collect data about denied application launches.
11. If required, modify the Applications Launch Control component operating mode.

12. When the period for gathering information about prevented application launches expires, make a selection from *Application startup prohibited* and *Application startup prohibited in test mode* events and export it to a TXT file. For details, refer to the "Event selections" section in the Kaspersky Security Center Help.

13. Open the exported TXT file.

14. If necessary, edit the list of events.

Added Applications Launch Control rules are displayed in the list.

9. If necessary, perform step 5 to add more Applications Launch Control rules.

10. If necessary, edit the added Applications Launch Control rules by clicking the **Edit** button.

11. If necessary, delete the added Applications Launch Control rules by clicking the **Delete** button.

12. Click **OK**.

How to add Applications Launch Control rules in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.

2. Click the **Properties** link in the results pane.
   The **Applications Launch Control** window opens on the **General** tab.

3. Select the **Rules** tab.

4. Add Applications Launch Control rules in any of the following ways:

   - **Manually**

     a. Click **Add**.
     The **Applications Launch Control** window opens.

     b. In the **Name** field, enter the name of the rule.

     c. If necessary, in the **Description** field, enter a description of the rule.

     d. In the **Type** drop-down list, select the rule type:

     - **Allowing** if you want the rule to allow running applications described by the rule.
     - **Denying** if you want the rule to block the launch of applications described by the rule.

     e. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

     - **Executable files**, if you want the rule to control launch of executable files.
     - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages. Files with the following extensions are supported: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Select the **Trusted Updaters** check box if you want Kaspersky Industrial CyberSecurity for Nodes to consider applications matching the rule trigger conditions as trusted updaters. Trusted Updaters are applications that are allowed to create other executable files that will be allowed to run subsequently.

If an application triggers multiple rules, Kaspersky Industrial CyberSecurity for Nodes sets the *Trusted Updaters* flag if the following conditions are satisfied:

- All rules allow the application to run.
- At least one rule has the **Trusted Updaters** check box selected.

g. Add trigger conditions for the Applications Launch Control rule.

h. Add exclusions from trigger conditions for the Applications Launch Control rule.

i. Add users and/or groups of users that are allowed or forbidden to launch applications that satisfy the rule.

j. Click **OK**.

- **By importing an XML file containing Applications Launch Control rules**

a. In the context menu of the button, select the **Import** → **From XML file** item.

b. Choose how to add Device Control rules from an XML file to those available in the policy:

- **Replace existing rules**, if you want to replace the existing rules with the imported rules.
- **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
- **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

c. In the window that opens, specify the path to the XML file that was created after the completion of local task or group task for *Rule Generator for Applications Launch Control*.

d. Click **Open**.

Added Applications Launch Control rules are displayed in the list.

5. If necessary, perform step 5 to add more Applications Launch Control rules.
6. If necessary, edit the added Applications Launch Control rules by clicking the **Edit** button.
7. If necessary, delete the added Applications Launch Control rules by clicking the **Delete** button.
8. Click **OK**.

How to add Applications Launch Control rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Local activity control** section.

5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.

6. Select the **Rules** tab.

7. In the **Application of rules** drop-down list, select the rule application mode:

   - **Add policy rules to the local rules**. The application applies the rule list specified in a policy together with local rule lists.

   - **Replace local rules with policy rules**. The application applies the rule list specified in the policy for application launch control on a group of protected devices. Local rule lists cannot be created, edited, or applied.

8. If necessary, enable the **Deny modification of local rules by users** functionality.

   If this functionality is enabled, the application does not allow editing Applications Launch Control rules locally in the Application Console. By default, the functionality is disabled.

9. Add Applications Launch Control rules in any of the following ways:

   - **Manually**

     a. Click **Add**.

        The **Rule settings** window opens.

     b. In the **Name** field, enter the name of the rule.

     c. In the **Type** drop-down list, select the rule type:

        - **Allowing** if you want the rule to allow running applications described by the rule.

        - **Denying** if you want the rule to block the launch of applications described by the rule.

     d. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

        - **Executable files**, if you want the rule to control launch of executable files.

        - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages.

     e. Select the **Deny for other users** check box if you want the application to block the launch of the applications described by the rule for all users that are not listed on the **User or group** tab.

     f. Select the **Trusted Updaters** check box if you want Kaspersky Industrial CyberSecurity for Nodes to consider applications matching the rule trigger conditions as trusted updaters. Trusted Updaters are applications that are allowed to create other executable files that will be allowed to run subsequently.

If an application triggers multiple rules, Kaspersky Industrial CyberSecurity for Nodes sets the *Trusted Updaters* flag if the following conditions are satisfied:

- All rules allow the application to run.
- At least one rule has the **Trusted Updaters** check box selected.

g. Add trigger conditions for the Applications Launch Control rule.

h. Add exclusions from trigger conditions for the Applications Launch Control rule.

i. **Add users and/or groups of users that are allowed or forbidden to launch applications that satisfy the rule**.

a. Select the **User or group** tab.

b. Click **Add**.

c. This opens a window; in that window, enter or select the name of a user or group of users.

d. Click **Select**.

e. Complete steps b through d for every user or group of users.

j. Click **OK**.

Added Applications Launch Control rules are displayed in the list.

- **By importing an XML file containing Applications Launch Control rules**

a. Click **Import**.

b. In the displayed **Import from file** window, click the **Select** button.

c. Specify the path to the XML file that was created after the completion of local task or group task for *Rule Generator for Applications Launch Control*.

d. Click **Open**.

e. Click **Import**.

Imported Applications Launch Control rules are added to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

- **By importing an XML file containing Kaspersky Industrial CyberSecurity for Nodes 4.0 Applications Launch Control rules**

a. Click **Import from the previous version**.

b. In the displayed **Import from file** window, click the **Select** button.

c. Specify the path to the XML file with Applications Launch Control rules that was exported from Kaspersky Industrial CyberSecurity for Nodes 4.0.

d. Click **Open**.

e. Click **Import**.

Imported Applications Launch Control rules are added to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

- **By importing rules from a Kaspersky Security Center report file**

  a. Click **Import from KSC report**.

  b. In the window that opens, select the TXT file into which the events from the report were exported.

  c. Click **Open**.

  Rules based on the Kaspersky Security Center report are added to the list of rules in the policy.

- **Based on Kaspersky Security Center events using a request**

  a. Click **Allowing rules from KSC events**.

  The **Rule Generator for Applications Launch Control** window opens.

  b. Select the type of events based on which the application will create Applications Launch Control rules:

  - **All events**.
  - **Application launch denied**.
  - **Statistics only mode: application launch denied**.

  c. Select a period from the **Use events generated within the period** drop-down list.

  d. Clear or select the **Prioritize the use of hash when generating rules** check box.

  If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes uses the checksum of the file to generate the rule when both the checksum and the certificate of the file are available.

  If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes uses the digital certificate of the file to generate the rule when both the checksum and the certificate of the file are available.

  e. If necessary, specify the name of the group of managed devices in the **Use events generated for a group of managed devices** field.

  f. Click **Generate rules**.

  g. From the **Rule for adding to the main list** drop-down list, select the principle for adding the rules to the list of previously created Application Launch Control rules:

  - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

h. Select rules that you want to export into Application Launch Control rules of the policy and click the **Export** button.

i. Save your changes.

10. If necessary, perform step 5 to add more Applications Launch Control rules.

11. If necessary, edit the added Applications Launch Control rules by clicking the **Edit** button.

12. If necessary, delete the added Applications Launch Control rules by clicking the **Delete** button.

13. Click **OK**.

Adding trigger conditions for the Applications Launch Control rule

How to add trigger conditions for the Applications Launch Control rule in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, go to the **Local activity control** section.

4. In the **Applications Launch Control** block, click the **Settings** button.
   The **Applications Launch Control** window opens on the **General** tab.

5. Select the **Rules** tab.

6. Do one of the following:

   a. Click the **Add** button if you are adding a new Applications Launch Control rule.

   b. In the list of Applications Launch Control rules, select the rule for which you want to add triggering conditions, and click the **Edit** button.

   The **Applications Launch Control** window opens.

7. On the **Conditions** tab, in the context menu of the **Add** button, select a triggering condition for the Applications Launch Control rule:

   - **Information from file**. **Information from the selected file** is used as the rule triggering condition.

     a. Click the **Browse** button in the **Information from file** window.
        The standard Microsoft Windows **Open File** window opens.

     b. Select the file.

     c. Click **Open**.
        Information about the selected file is displayed in the **Information from file** window.

d. Select at least one option:

- **Certificate details**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.
- **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.
- **File hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.
- **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

e. If necessary, in the **Command line** field, enter the command for starting the application on the command line. The rule controls the launch of this application. You can use ? and * characters to enter a mask.

> Kaspersky Industrial CyberSecurity for Nodes does not recognize paths that contain slashes ("/"). Use the backslash character ("\") in paths.

f. Click **OK**.

- **Drive type**. The rule controls the launch of applications from all removable drives connected to the protected computer.
- **KL category**. The rule controls the launch of applications that belong to the selected KL categories.
- **Trusted by KSN**. The rule controls the launch of applications that are trusted in KSN.
- **Untrusted by KSN**. The rule controls the launch of applications that are untrusted in KSN.
- **Trusted by OS**. The rule controls the launch of applications that are trusted in the operating system.

The added condition will be displayed in the list.

8. If necessary, perform the previous step of the instructions for each of the subsequent rule triggering conditions.
9. If necessary, edit rule triggering conditions by clicking the **Edit** button.
10. Save your changes.

How to add trigger conditions for the Applications Launch Control rule in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.
2. Click the **Properties** link in the results pane.

   The **Applications Launch Control** window opens on the **General** tab.
3. Select the **Rules** tab.

4. Do one of the following:

   a. Click the **Add** button if you are adding a new Applications Launch Control rule.

   b. In the list of Applications Launch Control rules, select the rule for which you want to add triggering conditions, and click the **Edit** button.

   The **Applications Launch Control** window opens.

5. On the **Conditions** tab, in the context menu of the **Add** button, select a triggering condition for the Applications Launch Control rule:

   - **Information from file**. **Information from the selected file** is used as the rule triggering condition.

     a. Click the **Browse** button in the **Information from file** window.

     The standard Microsoft Windows **Open File** window opens.

     b. Select the file.

     c. Click **Open**.

     Information about the selected file is displayed in the **Information from file** window.

     d. Select at least one option:

     - **Certificate details**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.
     - **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.
     - **File hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.
     - **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

     e. If necessary, in the **Command line** field, enter the command for starting the application on the command line. The rule controls the launch of this application. You can use ? and * characters to enter a mask.

     > Kaspersky Industrial CyberSecurity for Nodes does not recognize paths that contain slashes ("/"). Use the backslash character ("\") in paths.

     f. Click **OK**.

   - **Drive type**. The rule controls the launch of applications from all removable drives connected to the protected computer.
   - **KL category**. The rule controls the launch of applications that belong to the selected KL categories.
   - **Trusted by KSN**. The rule controls the launch of applications that are trusted in KSN.
   - **Untrusted by KSN**. The rule controls the launch of applications that are untrusted in KSN.
   - **Trusted by OS**. The rule controls the launch of applications that are trusted in the operating system.

The added condition will be displayed in the list.

6. If necessary, perform the previous step of the instructions for each of the subsequent rule triggering conditions.

7. If necessary, edit rule triggering conditions by clicking the **Edit** button.

8. Save your changes.

How to add trigger conditions for the Applications Launch Control rule in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Local activity control** section.

5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.

6. Select the **Rules** tab.

7. Click **Add**.

   The **Rule settings** window opens.

8. On the **Conditions** tab, click the **Add** button.

   The **Rule settings** window opens.

9. Select a triggering condition for the Applications Launch Control rule:

   - **Information from file**. **Information from the file** is used as the rule triggering condition.

     a. Under **Rule triggering criteria**, specify a value for at least one criterion:

     - **Digital certificate**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.

     - **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.

     - **SHA256 hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.

     - **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

     b. Click **OK**.

   - **From KL category**. The rule controls the launch of applications that belong to the selected KL categories.

- **Removable drive**. The rule controls the launch of applications from all removable drives connected to the protected computer.
- **Trusted by OS**. The rule controls the launch of applications that are trusted in the operating system.

The added condition will be displayed in the list.

10. If necessary, perform steps 4 through 5 of the instructions for each of the subsequent rule triggering conditions.
11. If necessary, edit rule triggering conditions by clicking the **Edit** button.
12. Save your changes.

Adding exclusions from an Applications Launch Control rule scope

How to add exclusions from the scope of the Applications Launch Control rule in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **Applications Launch Control** block, click the **Settings** button.
   The **Applications Launch Control** window opens on the **General** tab.
5. Select the **Rules** tab.
6. Do one of the following:
   a. Click the **Add** button if you are adding a new Applications Launch Control rule.
   b. In the list of Applications Launch Control rules, select the rule for which you want to add exclusions, and click the **Edit** button.

   The **Applications Launch Control** window opens.
7. On the **Exclusions** tab, in the context menu of the **Add** button, select a criterion for creating an exclusion from the scope of the Applications Launch Control rule:
   - **Information from file**. **Information from the selected file** is used as the criterion.
     a. Click the **Browse** button in the **Information from file** window.
        The standard Microsoft Windows **Open File** window opens.
     b. Select the file.
     c. Click **Open**.
        Information about the selected file is displayed in the **Information from file** window.

d. Select at least one option:

- **Certificate details**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.
- **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.
- **File hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.
- **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

e. If necessary, in the **Command line** field, enter the command for starting the application on the command line. The rule does not control the launch of this application. You can use ? and * characters to enter a mask.

> Kaspersky Industrial CyberSecurity for Nodes does not recognize paths that contain slashes ("/"). Use the backslash character ("\") in paths.

f. Click **OK**.

- **Drive type**. The rule does not control the launch of applications from all removable drives connected to the protected computer.
- **KL category**. The rule does not control the launch of applications that belong to the selected KL categories.
- **Trusted by KSN**. The rule does not control the launch of applications that are trusted in KSN.
- **Untrusted by KSN**. The rule does not control the launch of applications that are untrusted in KSN.
- **Trusted by OS**. The rule does not control the launch of applications that are trusted in the operating system.

The added exclusion will be displayed in the list.

8. If necessary, perform the previous step of the instructions to add each subsequent exclusion from the scope of the Applications Launch Control rule.
9. If necessary, edit exclusions by clicking the **Edit** button.
10. Save your changes.

How to add exclusions from the scope of the Applications Launch Control rule in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.
2. Click the **Properties** link in the results pane.

   The **Applications Launch Control** window opens on the **General** tab.
3. Select the **Rules** tab.

4. Do one of the following:

   a. Click the **Add** button if you are adding a new Applications Launch Control rule.

   b. In the list of Applications Launch Control rules, select the rule for which you want to add exclusions, and click the **Edit** button.

   The **Applications Launch Control** window opens.

5. On the **Exclusions** tab, in the context menu of the **Add** button, select a criterion for creating an exclusion from the scope of the Applications Launch Control rule:

   - **Information from file**. **Information from the selected file** is used as the criterion.

     a. Click the **Browse** button in the **Information from file** window.

     The standard Microsoft Windows **Open File** window opens.

     b. Select the file.

     c. Click **Open**.

     Information about the selected file is displayed in the **Information from file** window.

     d. Select at least one option:

     - **Certificate details**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.
     - **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.
     - **File hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.
     - **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

     e. If necessary, in the **Command line** field, enter the command for starting the application on the command line. The rule does not control the launch of this application. You can use ? and * characters to enter a mask.

     > Kaspersky Industrial CyberSecurity for Nodes does not recognize paths that contain slashes ("/"). Use the backslash character ("\") in paths.

     f. Click **OK**.

   - **Drive type**. The rule does not control the launch of applications from all removable drives connected to the protected computer.
   - **KL category**. The rule does not control the launch of applications that belong to the selected KL categories.
   - **Trusted by KSN**. The rule does not control the launch of applications that are trusted in KSN.

- **Untrusted by KSN**. The rule does not control the launch of applications that are untrusted in KSN.
- **Trusted by OS**. The rule does not control the launch of applications that are trusted in the operating system.

The added exclusion will be displayed in the list.

6. If necessary, perform the previous step of the instructions to add each subsequent exclusion from the scope of the Applications Launch Control rule.
7. If necessary, edit exclusions by clicking the **Edit** button.
8. Save your changes.

How to add exclusions from the scope of the Applications Launch Control rule in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Local activity control** section.
5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.
6. Select the **Rules** tab.
7. Click **Add**.

   The **Rule settings** window opens.
8. On the **Exclusions** tab, click the **Add** button.

   The **Rule settings** window opens.
9. Select a criterion for creating an exclusion from the scope of the Applications Launch Control rule:
   - **Information from file**. The rule does not control the launch of applications whose data matches the **data in the file**.

     a. Under **Rule triggering criteria**, specify a value for at least one criterion:

     - **Digital certificate**. If this check box is selected, the rule does not control the launch of applications signed with a digital certificate that has the specified data.
     - **Metadata**. If this check box is selected, the rule does not control the launch of applications that have the specified metadata.

- **SHA256 hash**. If this check box is selected, the rule does not control the launch of applications that have the specified SHA256 hash.
- **File path**. If this check box is selected, the rule does not control the launch of applications at the specified path.

b. Click **OK**.

- **KL category**. The rule does not control the launch of applications that belong to the selected KL categories.
- **Drive type**. The rule does not control the launch of applications from all removable drives connected to the protected computer.
- **Trusted by OS**. The rule does not control the launch of applications that are trusted in the operating system.

The added condition will be displayed in the list.

10. If necessary, perform steps 4 through 5 of the instructions to add each subsequent exclusion from the scope of the Applications Launch Control rule.
11. If necessary, edit exclusions by clicking the **Edit** button.
12. Save your changes.

Permitting all applications to run

You can allow launching all applications using specially configured Applications Launch Control allow rules.

To allow launching all applications:

1. Manually add two Applications Launch Control allow rules with the following parameters:
   - Rule type: *Allow*, Scope: *Executable files*, File path: `?:\`.
   - Rule type: *Allow*, Scope: *Scripts and MSI packages*, File path: `?:\`.
2. If Applications Launch Control deny rules have been added, delete these deny rules.
3. For all previously created Applications Launch Control allow rules, delete exclusions.
4. Save your changes.

Exporting Applications Launch Control rules

You can export the list of Applications Launch Control rules and the list of Software Distribution Control trusted installation packages to an XML file. You can use the export function to back up the list of Applications Launch Control rules or to migrate the list to a different server.

Exporting Applications Launch Control rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **Applications Launch Control** block, click the **Settings** button.

   The **Applications Launch Control** window opens on the **General** tab.
5. Go to the **Rules** tab to export Applications Launch Control rules, or to the **Software Distribution Control** tab to export Software Distribution Control rules.
6. If you want to export the entire list, click the button and select **Export**.
7. If you want to export only part of the list, follow these steps:

   a. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

   b. Click the button and select **Export selected**.
8. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

Exporting Applications Launch Control rules in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Application Console tree, select the **Computer Control** → **Applications Launch Control** section.
2. Click the **Properties** link in the results pane.

   The **Applications Launch Control** window opens on the **General** tab.
3. Go to the **Rules** tab to export Applications Launch Control rules, or to the **Software Distribution Control** tab to export Software Distribution Control rules.
4. If you want to export the entire list, click the button and select **Export**.
5. If you want to export only part of the list, follow these steps:

   a. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

   b. Click the button and select **Export selected**.
6. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

Exporting Applications Launch Control rules in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Local activity control** section.
5. In the **Applications Launch Control** block, click the **Configure** button.

   The **Applications Launch Control** window opens on the **General** tab.
6. Go to the **Rules** tab to export Applications Launch Control rules, or to the **Software Distribution Control** tab to export Software Distribution Control rules.
7. Using check boxes, select the rules that you want to export.
8. Click the **Export** button.This opens a window; in that window, specify whether you want to export selected rules or all rules, then click **Export**.

   If you did not select any rule, Kaspersky Industrial CyberSecurity for Nodes will export all rules.

Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

Generating a TXT file with a selection of Kaspersky Security Center blocked application events

You can export a selection of Kaspersky Security Center blocked application events to a TXT file and then import this data to generate a list of Applications Launch Control allow rules in a policy that you are configuring.

How to generate a TXT file with a selection of Kaspersky Security Center blocked application events using the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Logs and notifications** section.
4. In the **Task logs** block, click the **Settings** button.

   The **Notifications** window opens.
5. Expand the **Local activity control** node.
6. Select the **Applications Launch Control** section.
7. In the list of Applications Launch Control events, in the **Send events to Kaspersky Security Center** column, select check boxes next to *Application startup prohibited* and *Application startup prohibited in test mode*.
8. Save your changes.

9. In the **Event configuration** section of the policy, make sure that the event storage duration specified in the **Store in the Administration Server database for (days)** field is greater than the period for which you plan to gather information about prevented application launches (the default is 30 days).

   Once the Applications Launch Control component log retention period expires, logged events will be deleted and will not appear in the report.

10. Activate the policy configured to collect data about denied application launches.

11. If required, modify the Applications Launch Control component operating mode.

12. When the period for gathering information about prevented application launches expires, make a selection from *Application startup prohibited* and *Application startup prohibited in test mode* events and export it to a TXT file. For details, refer to the "Event selections" section in the Kaspersky Security Center Help.

13. Open the exported TXT file.

14. If necessary, edit the list of events.

How to generate a TXT file with a selection of Kaspersky Security Center blocked application events using the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Logs and notifications** section.

5. In the **Task logs** block, click the **Configure** button.

   The **Task logs** window opens.

6. Select the **Applications Launch Control** section.

7. In the list of Applications Launch Control events, in the **Send events to Kaspersky Security Center** column, select check boxes next to *Application startup prohibited* and *Application startup prohibited in test mode*.

8. Save your changes.

9. On the **Event configuration** tab of the policy that you are configuring, make sure that the event storage duration specified in the **Store in the Administration Server database for (days)** field is greater than the period for which you plan to gather information about prevented application launches (the default is 30 days).

   Once the Applications Launch Control component log retention period expires, logged events will be deleted and will not appear in the report.

10. Activate the policy configured to collect data about denied application launches.

11. If required, modify the Applications Launch Control component operating mode.

12. When the period for gathering information about prevented application launches expires, make a selection from *Application startup prohibited* and *Application startup prohibited in test mode* events and export it to a TXT file. For details, refer to the "Event selections" section in the Kaspersky Security Center Help.

13. Open the exported TXT file.

14. If necessary, edit the list of events.

Configuring Rule Generator for Applications Launch Control group task

How to configure the Rule Generator for Applications Launch Control group task in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

2. Select the administration group for which you want to configure the task.

3. Select the **Tasks** tab.

4. In the list of group tasks, open the *Rule Generator for Applications Launch Control* task by double-clicking the name of the task.

   The **Properties: Rule Generator for Applications Launch Control** window opens.

5. Go to the **Options** section.

6. If necessary, on the **Rules** tab, enter a prefix for rule names.

7. Under **Allowing rule usage scope**, specify the method you want to use for creating allow rules:

   - Create allowing rules based on running applications.
   - Create allowing rules for applications from the folders.

8. On the **Settings** tab, select the criterion that the task will apply when creating Applications Launch Control allow rules:

   - **Use digital certificate**.

     If this option is selected, the presence of a digital certificate is specified as a rule triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. Kaspersky Industrial CyberSecurity for Nodes will allow files that have a digital certificate. We recommend this option if you want to allow the start of any applications that are trusted in the operating system. This option is selected by default.

   - Use digital certificate subject and thumbprint.
   - If the certificate is missing, use.

- **Use SHA256 hash**.

  If this option is selected, the checksum of the file used to generate the rule is specified as a rule triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. Kaspersky Industrial CyberSecurity for Nodes will allow applications launched using files with a specified checksum. Using a SHA256 checksum as a rule triggering criterion restricts the rule usage scope to one file.

9. Configure the **Add a file path for rules generated based on hash sums** setting.

   If this check box is selected, when exporting rules, Kaspersky Industrial CyberSecurity for Nodes adds full paths to executable files to the XML file. The full paths can help you tell which software an executable file belongs to.

   If the check box is cleared, the XML file contains only names and SHA256 hashes of executable files. By default, the check box is cleared.

10. Add users and/or groups of users that will be allowed to launch applications that satisfy the rules created using the task:

    a. In the context menu of the **Add** button, select the method for adding users or groups.

    b. This opens a window; in that window, enter or select the name of a user or group of users.

    c. Click **OK**.

    d. Complete steps a through c for every user or group of users.

11. In the **After task completes** block, configure the following settings:

    - Add allowing rules to the list of Applications Launch Control rules.
    - Principle of adding.
    - **Export allowing rules to file**.
    - Add protected device details to the file name.

12. If necessary, on the **Exclusions** tab, specify objects that you want to exclude from the scope of the task.

13. Click the **OK** button in the **Properties: Rule Generator for Applications Launch Control** window.

How to configure the Rule Generator for Applications Launch Control group task in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

2. In the list of group tasks, open the Rule Generator for Applications Launch Control task.

   The **Rule Generator for Applications Launch Control** window opens.

3. Open the **Application settings** tab.

4. If necessary, in the **Allowing rule usage scope** section, enter a prefix for rule names.

5. Under **Allowing rule usage scope**, specify the method you want to use for creating allow rules:

   - Create allowing rules based on running applications
   - Create allowing rules for applications from the folders

6. On the **Parameters** tab, select the criterion that the task will apply when creating Applications Launch Control allow rules:

   - **Use digital certificate**.
   - **Use digital certificate subject and thumbprint**.
   - **If the certificate is missing, use**.
   - **Use SHA256 hash**.

7. Configure the **Add a file path for rules generated based on hash sums** setting.

   If this check box is selected, when exporting rules, Kaspersky Industrial CyberSecurity for Nodes adds full paths to executable files to the XML file. The full paths can help you tell which software an executable file belongs to.

   If the check box is cleared, the XML file contains only names and SHA256 hashes of executable files. By default, the check box is cleared.

8. Add users and/or groups of users that will be allowed to launch applications that satisfy the rules created using the task:

   a. Click **Add user or group**.

   b. This opens a window; in that window, enter or select the name of a user or group of users.

   c. Click **Select**.

   d. Complete steps a through c for every user or group of users.

9. In the **After task completes** block, configure the following settings:

   - **Add allowing rules to the list of Applications Launch Control rules**.
   - **Principle of adding**.
   - **The allowing rules will be exported to a file**. In the **Specify the full path to a file with .xml extension** field, you can specify a path to which Kaspersky Industrial CyberSecurity for Nodes will export allow rules to an XML file when the Rule Generator for Applications Launch Control task finishes.
   - **Add protected device details to the file name**.

10. If necessary, on the **Exclusions** tab, specify objects that you want to exclude from the scope of the task.

11. Click the **OK** button in the **Rule Generator for Applications Launch Control** window.

Creating rules using a Rule Generator for Applications Launch Control group task.

To create rules using a Rule Generator for Applications Launch Control group task:

1. Create a *Rule Generator for Applications Launch Control* group task or select an existing task.
2. Configure the Rule Generator for Applications Launch Control task.
3. Run the Rule Generator for Applications Launch Control task.

After the task finishes, depending on task settings:

- If you specified the **Add allowing rules to the list of Applications Launch Control rules** action on task completion, the generated Applications Launch Control rules are added to the list in Applications Launch Control settings in the Application Console.
- If you specified the **The allowing rules will be exported to a file** action on task completion, the generated Applications Launch Control rules are saved to an XML file at the path specified in task settings.

The lists contain allowing rules for launching applications whose type matches the settings of the Rule Generator for Applications Launch Control group task.

Device Control

Device Control manages user access to devices that are installed on or connected to a computer (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the computer from infection when such devices are connected, and prevent data loss or data leaks.

Device Control provides the following functionality:

- Managing user access permissions to storage devices (for example, removable drives, mobile phones, CD/DVD drives, and so on).
- Controlling the connection of devices without a file system (for example, external modems, Bluetooth adapters, USB keyboards, and so on).
- Managing Wi-Fi connections.

By default, Device Control is disabled. When you enable Device Control, Kaspersky Industrial CyberSecurity for Nodes denies access by default to the following device types:

- Removable drives (including USB flash drives)
- Floppy disks
- CD/DVD drives
- Portable devices (MTP)
- Modems.
- Smart card readers
- External network adapters
- Bluetooth (except input devices)

Device Control levels

Kaspersky Industrial CyberSecurity for Nodes controls device access on the following levels:

1. **Device type**.

   When connecting a device to the computer, the operating system determines the type of the device: printer, removable drive, CD/DVD drive, and so on. On this level, you can allow or deny the connection of devices by type.

2. **Connection bus**.

   A *connection bus* is an interface used for connecting devices to the computer. Some device types have multiple connection interfaces. For example, you can connect a printer to USB or serial (COM) port.

   At this level, you can allow or deny access to devices depending on connection bus.

For example, suppose you denied access via USB. Kaspersky Industrial CyberSecurity for Nodes denies access to all device types with **Depends on connection bus** mode when connected via USB.

> If the **Allow** or **Block** access mode is selected for the device, access control disregards the connection bus of the device.

3. **Trusted devices**.

   Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

Device Control operating modes

Device Control can work in the following modes:

- **Active mode**.

  Kaspersky Industrial CyberSecurity for Nodes denies or allows devices based on configured device access rules. The application also allows access to trusted devices. The application registers device connection and disconnection events.

- **Inform**.

  Kaspersky Industrial CyberSecurity for Nodes allows all devices and logs corresponding events. All devices are allowed. This mode is set by default. You can enable this mode to conduct an audit of devices in your organization and use this information to draft a list of trusted devices.

Device Access Rules

A *device access rule* is a group of settings that determine how users can access devices that are installed or connected to the computer. These settings include access to a specific device, an access schedule, read or write permissions and others. The group of settings for an access rule differs depending on the type of device.

Access rule settings

Devices	Assignment of users and/or a group of users	Schedule for access to a device	Read/write permission	Connection bus monitoring
Hard drives	✓	✓	✓	✓
Removable drives (including USB flash drives)	✓	✓	✓	✓
Floppy disks	✓	✓	✓	✓
CD/DVD drives	✓	✓	✓	✓
Portable devices (MTP)	✓	✓	✓	✓
Local printers	✓	–	–	✓
Network printers	✓	–	–	–
Modems	–	–	–	✓
Streamers	–	–	–	✓
Multifunctional devices	–	–	–	✓
Smart card readers	–	–	–	✓

Devices	Assignment of users and/or a group of users	Schedule for access to a device	Read/write permission	Connection bus monitoring
Windows CE USB ActiveSync devices	–	–	–	✓
External network adapters	–	–	–	✓
Bluetooth	–	–	–	–
Cameras and scanners	–	–	–	✓
Wi-Fi	–	–	–	–
USB keyboards	–	–	–	✓
USB mice	–	–	–	✓

Managing access to devices by type

Device Control allows managing access to devices by type. The type of the device is determined by the operating system when the device is connected. You can look up the device type using the Device Manager tool built into the operating system. To manage access to devices, you must configure rules. A *device access rule* is a group of settings that determine how users can access devices that are installed or connected to the computer. These settings include access to a specific device, an access schedule, read or write permissions and others. The group of settings for an access rule differs depending on the type of device.

You can configure device access as follows:

- **Allow**.

  Kaspersky Industrial CyberSecurity for Nodes grants full access to devices to all users.

- **Block**.

  Kaspersky Industrial CyberSecurity for Nodes blocks device connection. The application allows connecting only trusted devices.

- **Depends on connection bus**.

  Kaspersky Industrial CyberSecurity for Nodes identifies the connection bus of the device and performs access control in accordance with the access mode of the connection bus. The application also allows connecting trusted devices.

- **By rules**.

  For some device types, you can select users or a group of users that will be allowed to use devices, configure a device access schedule, and read and write permissions. The application also allows connecting trusted devices.

Be careful when configuring access to devices of the **Hard drives** type. If you block access to the system disk, the application may cause a crash (BSOD) when booting the operating system.

If a device does not fit in the Device Control classification scheme, access to such a device cannot be restricted.

How to control access to devices by type in Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.
8. Configure the device access rules:

   a. Select access mode: **Allow**, **Block**, **Depends on connection bus**, **By rules**.

   To select the **By rules** access mode, you must double-click to open access rule properties.

   b. If you selected the **Depends on connection bus** access mode, go to the **Connection buses** tab and configure access rules for connection interfaces.

   c. For storage devices (for example, removable drives), you can configure access rights of individual users. You can also configure a device access schedule and configure read and write permissions.

   d. If necessary, configure the printing rules.

   e. If necessary, configure Wi-Fi connection rules.
9. Save your changes. To apply the policy on computers, close the padlocks.

How to control access to devices by type in Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.
5. Select the **Enable Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.
8. Configure the device access rules:

   a. Select access mode: **Allow**, **Block**, **Depends on connection bus**, **By rules**.

   If the access mode is not available in the drop-down menu, open the properties of the access rule by double-clicking the device type.

b. If you select the **Depends on connection bus** access mode, you must go back to the window with general Device Control settings, click **Connection buses**, and configure access rules for connection interfaces.

c. For storage devices (for example, removable drives), you can configure access rights of individual users. You can also configure a device access schedule and configure read and write permissions.

d. If necessary, configure the printing rules.

e. If necessary, configure Wi-Fi connection rules.

9. Save your changes. To apply the policy on computers, close the padlocks.

How to control device access by type in Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.

2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.

3. Select the **Device Control** check box.

4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

5. Under **Device Control settings**, select the **Types of devices** tab.

   A window opens with access rules for all devices that are included in the Device Control component classification.

6. Configure the device access rules:

   a. Select access mode: **Allow**, **Block**, **Depends on connection bus**, **By rules**.

   To select the **By rules** access mode, you must double-click to open access rule properties.

   b. If you select the **Depends on connection bus** access mode, you must configure access rules for connection interfaces on the **Connection buses** tab.

   c. For storage devices (for example, removable drives), you can configure access rights of individual users. You can also configure a device access schedule and configure read and write permissions.

   d. If necessary, configure the printing rules.

   e. If necessary, configure Wi-Fi connection rules.

7. Save your changes.

As a result, when a user attempts to gain access to a device, the application blocks access in accordance with the rules. Kaspersky Industrial CyberSecurity for Nodes also logs the corresponding event. If you want to grant access to individual devices, you can add these devices to the list of trusted devices.

Control of Wi-Fi connections

Device Control allows managing the Wi-Fi connection of the computer (terminal). Public Wi-Fi networks may be insecure, and using such networks can result in data loss. Device Control lets you block a user from connecting to Wi-Fi or allow connecting only to trusted networks. For example, you can allow connecting only to the corporate Wi-Fi network that is sufficiently secure. Device Control will block access to all Wi-Fi networks except those specified in the trusted list.

On computers running Windows 11, you need to enable Location services in order to control Wi-Fi connections. To do this, you need to enable the **Location services** switch in the operating system settings (**Settings** → **Privacy & security** → **Location**). If Location services are disabled, Kaspersky Industrial CyberSecurity for Nodes does not control connections to Wi-Fi networks.

How to restrict Wi-Fi connections in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.
8. For **Wi-Fi** devices, configure an access rule:

   a. Select an access mode: **Allow**, **Block**, **Block with exceptions**.

   b. If you selected the **Block with exceptions** mode, you must create a list of trusted Wi-Fi networks:

      1. Double-click the **Wi-Fi** device type to open the list of trusted Wi-Fi networks.
      2. In the window that opens, click the **Add** button.
      3. This opens a window; in that window, configure the trusted Wi-Fi network:

         - **Network name**. Name or SSID (Service Set Identifier) of the Wi-Fi network.
         - **Authentication type**. Authentication type used when connecting to the Wi-Fi network.
         - **Encryption type**. Encryption type used to protect the Wi-Fi traffic.
         - **Comment**. Further info about the added Wi-Fi network.

You can view the settings of the trusted Wi-Fi network in router settings.

> A Wi-Fi network is considered trusted if its settings match all settings specified in the rule.

9. Save your changes. To apply the policy on computers, close the padlocks.

How to restrict Wi-Fi connections in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.
5. Select the **Enable Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.
8. Double-click the **Wi-Fi** device type to open access rule properties.
9. Select an access mode: **Allow**, **Block**, **Block with exceptions**.
10. If you selected the **Block with exceptions** mode, you must create a list of trusted Wi-Fi networks:
    1. In the **Trusted Wi-Fi networks** block, click the **Add** button.
    2. This opens a window; in that window, configure the trusted Wi-Fi network:
       - **Network name**. Name or SSID (Service Set Identifier) of the Wi-Fi network.
       - **Authentication type**. Authentication type used when connecting to the Wi-Fi network.
       - **Encryption type**. Encryption type used to protect the Wi-Fi traffic.
       - **Comment**. Further info about the added Wi-Fi network.

    You can view the settings of the trusted Wi-Fi network in router settings.

    > A Wi-Fi network is considered trusted if its settings match all settings specified in the rule.

11. Save your changes. To apply the policy on computers, close the padlocks.

How to restrict Wi-Fi connections in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.
3. Select the **Device Control** check box.
4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
5. Under **Device Control settings**, select the **Types of devices** tab.

   A window opens with access rules for all devices that are included in the Device Control component classification.
6. For **Wi-Fi** devices, configure an access rule:

   a. Select an access mode: **Allow**, **Block**, **Block with exceptions**.

   b. If you selected the **Block with exceptions** mode, you must create a list of trusted Wi-Fi networks:

      1. Double-click the **Wi-Fi** device type to open the list of trusted Wi-Fi networks.
      2. In the window that opens, click the **Add** button.
      3. This opens a window; in that window, configure the trusted Wi-Fi network:

         - **Network name**. Name or SSID (Service Set Identifier) of the Wi-Fi network.
         - **Authentication type**. Authentication type used when connecting to the Wi-Fi network.
         - **Encryption type**. Encryption type used to protect the Wi-Fi traffic.
         - **Comment**. Further info about the added Wi-Fi network.

   You can view the settings of the trusted Wi-Fi network in router settings.

   > A Wi-Fi network is considered trusted if its settings match all settings specified in the rule.
7. Save your changes.

As a result, when a user tries connecting to a Wi-Fi network that is not listed as trusted, the application blocks the connection.

Control of printing

Device Control allows configuring user access to local and network printers.

Local printer control

Kaspersky Industrial CyberSecurity for Nodes controls local printer connection over the following buses: USB, Serial Port (COM), Parallel Port (LPT).

> Kaspersky Industrial CyberSecurity for Nodes controls the connection of local printers to COM and LPT ports only on the level of the bus. That is, to prevent the connection of printers to COM and LPT ports, for the **Local printers** device type, select the **Depends on connection bus** mode and prohibit the connection of devices to COM and LPT buses.

For printers connected to USB, the application exercises control on two levels: device type (local printers) and connection bus (USB).

You can select one of the following access modes to local printers via USB:

- **Allow**. Kaspersky Industrial CyberSecurity for Nodes grants full access to local printers to all users. Users can connect printers and print documents using the means that the operating system provides.
- **Block**. Kaspersky Industrial CyberSecurity for Nodes blocks the connection of local printers. The application allows connecting only trusted printers.
- **Depends on connection bus**. Kaspersky Industrial CyberSecurity for Nodes allows connecting to local printers in accordance with the USB bus connection status (**Allow** or **Block**).
- **By rules**. To control printing, you must add *printing rules*. In the rules, you can select users or a group of users for which you want to allow or block access to printing documents on local printers.

Network printer control

Kaspersky Industrial CyberSecurity for Nodes allows configuring access to printing on network printers. You can select one of the following access modes to network printers:

- **Allow and do not log** . Kaspersky Industrial CyberSecurity for Nodes does not control printing on network printers. The application grants access to printing to all users and does not save information about printing to the event log.
- **Allow** . Kaspersky Industrial CyberSecurity for Nodes grants access to printing on network printers to all users.
- **Block** . Kaspersky Industrial CyberSecurity for Nodes restricts access to network printers for all users. The application allows access only to trusted printers.
- **By rules**. To control printing, you must add *printing rules*. In the rules, you can select users or a group of users for which you want to allow or block access to printing documents on network printers.

Adding printing rules for printers

How to add printing rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.
8. Configure the printer access rules:

   a. For **Local printers** and **Network printers** device types, configure access rules: **Allow**, **Block**, **Allow and do not log** (only for network printers), **Depends on connection bus** (only for local printers), **By rules**.

   b. If you selected the **Depends on connection bus** access mode, go to the **Connection buses** tab and configure access rules for connection interfaces.

   c. If you select the **By rules** access mode, you must configure printing rules:

      1. Double-click the **Local printers** and **Network printers** device type to open access rule properties.
      2. Select the users or groups of users to which you want to apply the printing rule. To do so, click the **Add** button.

         This opens a window for adding a new printing rule.
      3. Assign a priority to the *rule entry*. A rule entry includes the following attributes: user account, action (allow/block), and priority.

         A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

         For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

         The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.
      4. Under **Action**, configure user access to printing on the printer.

5. Click **Users and groups** and select users or groups of users for access to printing. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

6. Click **OK**.

9. Save your changes. To apply the policy on computers, close the padlocks .

How to add printing rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.

5. Select the **Enable Device Control** check box.

6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.

8. Configure the printer access rules:

   a. For **Local printers** and **Network printers** device types, select an access mode: **Allow**, **Block**, **Allow and do not log** (only for network printers), **Depends on connection bus** (only for local printers), **By rules**.

   If the access mode is not available in the drop-down menu, open the properties of the access rule by double-clicking the device type.

   b. If you select the **Depends on connection bus** access mode, you must go back to the window with the Device Control component general settings, click **Connection buses**, and configure access rules for connection interfaces.

   c. If you need to configure printing:

      1. Double-click the **Local printers** or **Network printers** device type to open access rule properties.

      2. Select the **By rules** access mode.

      3. Select the users or groups of users to which you want to apply the printing rule. To do so, click the **Add** button.

         This opens a window for adding a new printing rule.

      4. Assign a priority to the *rule entry*. A rule entry includes the following attributes: user account, action (allow/block), and priority.

A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

5. Under **Action**, configure user access to printing on the printer.

6. Under **Users and groups**, click **Add** and select users or groups of users for access to printing. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

7. Click **OK**.

9. Save your changes. To apply the policy on computers, close the padlocks.

How to add printing rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.

2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.

3. Select the **Device Control** check box.

4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

5. Under **Device Control settings**, select the **Types of devices** tab.

   A window opens with access rules for all devices that are included in the Device Control component classification.

6. Configure the printer access rules:

   a. For **Local printers** and **Network printers** device types, configure access rules: **Allow**, **Block**, **Allow and do not log** (only for network printers), **Depends on connection bus** (only for local printers), **By rules**.

   b. If you selected the **Depends on connection bus** access mode, go to the **Connection buses** tab and configure access rules for connection interfaces.

   c. If you select the **By rules** access mode, you must configure printing rules:

      1. Double-click the **Local printers** and **Network printers** device type to open access rule properties.

      2. Select the users or groups of users to which you want to apply the printing rule. To do so, click the **Add** button.

         This opens a window for adding a new printing rule.

3. Assign a priority to the *rule entry*. A rule entry includes the following attributes: user account, action (allow/block), and priority.

   A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

   For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

   The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

4. Under **Action**, configure user access to printing on the printer.

5. Click **Users and groups** and select users or groups of users for access to printing. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

6. Click **OK**.

7. Save your changes.

Input device control (HID)

Input devices include keyboards, mice, trackballs, touchpads, and other such devices. You can connect input devices using the following interfaces: USB, Bluetooth, PS/2 port, RS-232 (COM) port, IR port, etc.

Kaspersky Industrial CyberSecurity for Nodes allows controlling USB and Bluetooth mice and keyboards. Device Control logs input device connection and disconnection devices.

> When Bluetooth devices are connected or disconnected, the application may create multiple events about the device. The reason is that the operating system may detect a Bluetooth device as multiple devices of different types. Kaspersky Industrial CyberSecurity for Nodes also manages the Bluetooth adapter through which the device is connected as a separate device. That is why the application creates an event for each of the detected devices.

Kaspersky Industrial CyberSecurity for Nodes lets you allow or prohibit using an input device, as well as make a list of trusted devices.

How to enable Device Control in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, select **Local activity control**.

4. In the **Device Control** section, click **Settings**.

5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.
8. For the **Bluetooth** device type, select an access mode: **Allow**, **Block**, **Allow and do not log**.

   You can block or allow all Bluetooth devices or you can allow connecting only Bluetooth input devices (HID (Human Interface Devices) class).

   > You can allow connecting input devices only in the Kaspersky Security Center Web Console. You cannot allow connecting input devices in Administration Console (MMC) or Kaspersky Industrial CyberSecurity for Nodes Console.
9. For **USB keyboards** and **USB mice** device types, select an access mode: **Allow**, **Block**, **Depends on connection bus**.
10. Save your changes. To apply the policy on computers, close the padlocks.

How to enable Device Control in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.
5. Select the **Enable Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.
8. Click the **Bluetooth** device type to open access rule properties.
9. Select an access mode: **Allow**, **Block**, **Allow and do not log**.

   You can block or allow all Bluetooth devices or you can allow connecting only Bluetooth input devices (HID (Human Interface Devices) class).
10. For **USB keyboards** and **USB mice** device types, select an access mode: **Allow**, **Block**, **Depends on connection bus**.
11. Save your changes. To apply the policy on computers, close the padlocks.

How to configure Device Control in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.
3. Select the **Device Control** check box.
4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
5. Under **Device Control settings**, select the **Types of devices** tab.

   A window opens with access rules for all devices that are included in the Device Control component classification.
6. For the **Bluetooth** device type, select an access mode: **Allow**, **Block**, **Allow and do not log**.

   You can block or allow all Bluetooth devices or you can allow connecting only Bluetooth input devices (HID (Human Interface Devices) class).

   > You can allow connecting input devices only in the Kaspersky Security Center Web Console. You cannot allow connecting input devices in Administration Console (MMC) or Kaspersky Industrial CyberSecurity for Nodes Console.
7. For **USB keyboards** and **USB mice** device types, select an access mode: **Allow**, **Block**, **Depends on connection bus**.
8. Save your changes.

Managing access to mobile devices

Kaspersky Industrial CyberSecurity for Nodes allows you to control access to data on mobile devices running Android and iOS. Mobile devices belong to the category of portable devices (MTP). Therefore, to configure data access on mobile devices, you need to edit the access settings for portable devices (MTP).

When a mobile device is connected to the computer, the operating system determines the device type. If iTunes or similar applications are installed on the computer Android Debug Bridge (for more information about the ADB application, see the Knowledge Base and the Android Technical Support website), the operating system identifies mobile devices as ADB or iTunes devices. In all other cases, the operating system may identify the mobile device type as a portable device (MTP) for file transfer, a PTP device (camera) for image transfer, or another device. The device type depends on the model of the mobile device and the selected USB connection mode. Kaspersky Industrial CyberSecurity for Nodes lets you configure individual access permissions for data on mobile devices in ADB applications, iTunes, or the file manager. In all other cases, Device Control allows access to mobile devices in accordance with portable devices (MTP) access rules.

Access to mobile devices

Mobile devices belong to the category of portable devices (MTP), therefore the settings for them are the same. You can select one of the following modes of access to mobile devices:

- **Allow**. Kaspersky Industrial CyberSecurity for Nodes grants full access to mobile devices. You can open, create, modify, copy, or delete files on mobile devices using the file manager or the ADB and iTunes applications. You can also charge the battery of the device by connecting the mobile device to a USB port of the computer.
- **Block**. Kaspersky Industrial CyberSecurity for Nodes restricts access to mobile devices in the file manager and in the ADB and iTunes applications. The application allows access only to trusted mobile devices. You can also charge the battery of the device by connecting the mobile device to a USB port of the computer.
- **Depends on connection bus**. Kaspersky Industrial CyberSecurity for Nodes allows connecting to mobile devices in accordance with the USB bus connection status (**Allow** or **Block**).
- **By rules**. Kaspersky Industrial CyberSecurity for Nodes restricts access to mobile devices in accordance with the rules. In the rules, you can configure access permissions (read/write), select users or a group that have access to mobile devices, and configure a schedule for access to mobile devices. You can also restrict access to data on mobile devices via the ADB and iTunes applications.

Configuring mobile device access rules

Access rules for portable devices (MTP), ADB devices, and iTunes devices are configured differently. For portable devices (MTP) and ADB devices, you can configure rules for individual users or groups of users and create a schedule for when the rules will apply. For iTunes devices, you cannot do that. You can only allow or deny access to data through the iTunes application for all users.

How to configure mobile device access rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Under **Device Control settings**, select the **Types of devices** tab.

   The table lists access rules for all devices that are present in the classification of the Device Control component.
6. In the context menu for the **Portable devices (MTP)** device type, configure the mobile device access mode: **Allow**, **Block**, or **Depends on connection bus**.
7. To configure mobile device access rules, double-click to open the list of rules.

8. Configure the mobile device access rule:

   a. In the **Access rules** block, click the **Add** button.

      This opens a window for adding a new mobile device access rule.

   b. In the **Priority** field, set the rule write priority. A rule includes the following attributes: user account, schedule, permissions (read / write / ADB access), and priority.

      A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

      For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

      The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

   c. Under **Rule for users and groups**, select users or groups of users. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

   d. Click **OK**.

9. Under **Schedules for the selected access rule**, configure a mobile device access schedule for users.

   Configuring a separate access schedule for ADB devices is not possible. You can configure a common access schedule for ADB devices and portable devices (MTP).

10. Configure users' access permissions to mobile devices in the file manager (**Read** / **Write**).

11. Configure the access to data on a mobile device through the ADB application using the **Access via ADB** check box.

    If the check box is cleared, when the mobile device is connected, the ADB application is prevented from detecting the device.

12. Under **Access via iTunes**, configure access to data on the mobile device through the iTunes application.

    Kaspersky Industrial CyberSecurity for Nodes applies the settings for mobile device access through the iTunes application for all users. Configuring a separate access schedule for iTunes devices is not possible.

13. Save your changes.

How to configure mobile device access rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.

5. In the **Device Control Settings** block, click the **Access rules for devices and Wi-Fi networks** link.

   The table lists access rules for all devices that are present in the classification of the Device Control component.

6. Select the **Portable devices (MTP)** device type.

   This opens portable devices (MTP) access rights.

7. Configure the mobile devices access mode: **Allow**, **Block**, **Depends on connection bus**, or **By rules**.

8. Under **Access via iTunes**, configure access to data on the mobile device through the iTunes application.

   > Kaspersky Endpoint Security applies the settings for mobile device access through the iTunes application for all users. Configuring a separate access schedule for iTunes devices is not possible.

9. If you select the **By rules** mode, you must add access rules for devices. To do so, under **Users**, click the **Add** button and configure the mobile device access rule:

   a. In the **Priority** field, set the rule write priority. A rule includes the following attributes: user account, schedule, permissions (read / write / ADB access), and priority.

      A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

      For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

      The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

   b. Under **Users**, select users or groups of users for access to mobile devices. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

   c. Under **Schedule for access to devices**, configure a mobile device access schedule for users.

      > Configuring a separate access schedule for ADB devices is not possible. You can configure a common access schedule for ADB devices and portable devices (MTP).

   d. Configure users' access permissions to mobile devices in the file manager (**Read** / **Write**).

e. Configure the access to data on a mobile device through the ADB application using the **Access via ADB** check box.

If the check box is cleared, when the mobile device is connected, the ADB application is prevented from detecting the device.

10. Save your changes.

How to configure mobile device access rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.

2. In the results pane of the **Device Control** node, click **Properties**.

The **Properties: Device Control** window opens.

3. Select the **Types of devices** tab.

A window opens with access rules for all devices that are included in the Device Control component classification.

4. In the context menu for the **Portable devices (MTP)** device type, configure the mobile device access mode: **Allow**, **Block**, or **Depends on connection bus**.

5. To configure mobile device access rules, double-click to open the list of rules.

6. Configure the mobile device access rule:

a. In the **Access rules** block, click the **Add** button.

This opens a window for adding a new mobile device access rule.

b. In the **Priority** field, set the rule write priority. A rule includes the following attributes: user account, schedule, permissions (read / write / ADB access), and priority.

A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

c. Under **Rule for users and groups**, select users or groups of users. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

d. Click **OK**.

7. Under **Schedules for the selected access rule**, configure a mobile device access schedule for users.

Configuring a separate access schedule for ADB devices is not possible. You can configure a common access schedule for ADB devices and portable devices (MTP).

8. Configure users' access permissions to mobile devices in the file manager (**Read** / **Write**).

9. Configure the access to data on a mobile device through the ADB application using the **Access via ADB** check box.

   If the check box is cleared, when the mobile device is connected, the ADB application is prevented from detecting the device.

10. Under **Access via iTunes**, configure access to data on the mobile device through the iTunes application.

    Kaspersky Industrial CyberSecurity for Nodes applies the settings for mobile device access through the iTunes application for all users. Configuring a separate access schedule for iTunes devices is not possible.

11. Save your changes.

As a result, user access to mobile devices is restricted in accordance with rules. If you have prohibited access to mobile devices in the ADB and iTunes applications, when you connect a mobile devices, the ADB and iTunes applications are prevented from detecting the mobile device.

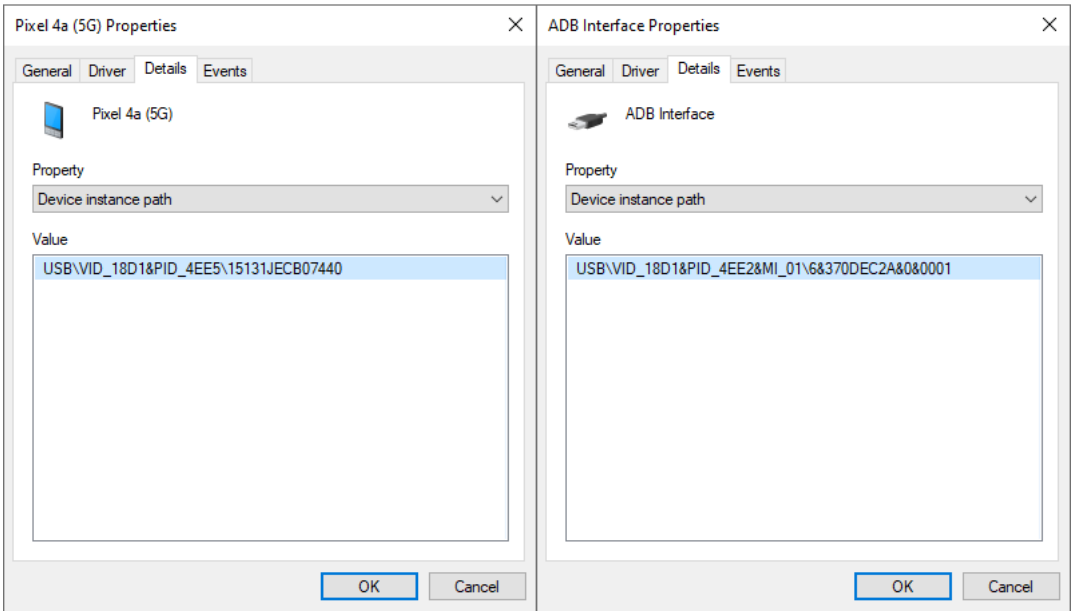
Trusted mobile devices

The procedure for adding a trusted mobile device is exactly the same as for other types of trusted devices. You can add a mobile device by ID or by device model.

To add a trusted mobile device by ID, you will need a unique ID (Hardware ID – HWID). You can find the ID in device properties by using operating system tools (see figure below). The Device Manager tool lets you do this. IDs of portable devices (MTP) and ADB, iTunes devices are different even for the same mobile device. The ID of a portable device (MTP) may look like this: `15131JECB07440`. The ID of an ADB device may look like this: `6&370DEC2A&0&0001`. Adding devices by ID is convenient if you want to add several specific devices. You can also use masks.

If you installed the ADB or iTunes applications after connecting a device to the computer, the unique ID of the device may be reset. That is, Kaspersky Industrial CyberSecurity for Nodes identifies this device as new. If a device is trusted, add the device to the trusted list again.

To add a trusted mobile device by device model, you will need its Vendor ID (VID) and Product ID (PID). You can find the IDs in device properties by using operating system tools (see figure below). Template for entering the VID and PID: `VID_18D1&PID_4EE5`. Adding devices by model is convenient if you use devices of a certain model in your organization. This way, you can add all devices of this model.



Device ID in Device Manager

Monitoring usage of removable drives

Monitoring usage of removable drives includes:

- Monitoring operations on files on removable drives.
- Monitoring connection and disconnection of trusted removable drives.

  Kaspersky Industrial CyberSecurity for Nodes allows monitoring connection and disconnection of all trusted devices and not only removable drives. You can turn on event logging in notification settings for the Device Control component. Events have the *Informational* severity level.

How to enable monitoring of file operations on removable drives in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.

8. Select the **Removable drives** device type and click the **Logging** button.

   This opens the event logging window.

9. Select the **Enable logging** check box.

10. In the **File operations** block, select the operations that you want to monitor: **Write**, **Delete**.

11. In the **Filter by file formats** block, select the formats of files whose associated operations should be logged by Device Control.

12. Select the users or group of users whose use of removable drives you want to monitor.

13. Save your changes. To apply the policy on computers, close the padlocks.

How to enable monitoring of file operations on removable drives in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.

5. Select the **Enable Device Control** check box.

6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.

8. Double-click the **Removable drives** device type to open access rule properties.

9. In the window that opens, select the **Logging** tab.

10. Set the toggle switch to **Logging ENABLED**.

11. In the **File operations** block, select the operations that you want to monitor: **Write**, **Delete**.

12. In the **Filter by file formats** block, select the formats of files whose associated operations should be logged by Device Control.

13. Select the users or group of users whose use of removable drives you want to monitor.

14. Save your changes. To apply the policy on computers, close the padlocks.

How to enable monitoring of file operations on removable drives in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.
3. Select the **Device Control** check box.
4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
5. Under **Device Control settings**, select the **Types of devices** tab.

   A window opens with access rules for all devices that are included in the Device Control component classification.
6. Select the **Removable drives** device type and click the **Logging** button.

   This opens the event logging window.
7. Select the **Enable logging** check box.
8. In the **File operations** block, select the operations that you want to monitor: **Write**, **Delete**.
9. In the **Filter by file formats** block, select the formats of files whose associated operations should be logged by Device Control.
10. Select the users or group of users whose use of removable drives you want to monitor.
11. Save your changes.

As a result, when users write to files located on removable drives or delete files from removable drives, Kaspersky Industrial CyberSecurity for Nodes will save information about such operations to the event log and send events to Kaspersky Security Center. You can view events associated with files on removable drives in the Kaspersky Security Center Console in the workspace of the **Administration Server** node on the **Events** tab. For events to be displayed in the local Kaspersky Industrial CyberSecurity for Nodes event log, you must select the **File operation performed** check box in the notifications settings for the Device Control component.

Managing access to Bluetooth devices

Kaspersky Industrial CyberSecurity for Nodes allows managing access to Bluetooth devices. Bluetooth devices include wireless keyboards, mice, headsets, printers, etc. You can also uses Bluetooth for communication e.g. with a mobile device.

When Bluetooth devices are connected or disconnected, the application may create multiple events about the device. The reason is that the operating system may detect a Bluetooth device as multiple devices of different types. Kaspersky Industrial CyberSecurity for Nodes also manages the Bluetooth adapter through which the device is connected as a separate device. That is why the application creates an event for each of the detected devices.

You can select one of the following modes of access to Bluetooth devices:

- **Allow and do not log** . Kaspersky Industrial CyberSecurity for Nodes allows connecting any Bluetooth devices and does not save information about the connection in the event log. You can connect Bluetooth input devices (keyboards, mice, etc), send data over Bluetooth, manage other Bluetooth devices (headset, headphones, etc).
- **Allow** . Kaspersky Industrial CyberSecurity for Nodes allows connecting any Bluetooth devices. You can connect Bluetooth input devices (keyboards, mice, etc), send data over Bluetooth, manage other Bluetooth devices (headset, headphones, etc).
- **Block** . Kaspersky Industrial CyberSecurity for Nodes restricts access to Bluetooth devices. You can allow connecting only Bluetooth input devices (the Human Interface Devices class). These devices include keyboards, mice, joysticks, etc.

It is not possible to create a list of trusted Bluetooth devices. If you have restricted access to Bluetooth devices, you can only connection of Bluetooth input devices.

You can allow connecting input devices only in the Application Console or in Kaspersky Security Center Web Console. You cannot allow connecting input devices in the Kaspersky Security Center Administration Console.

How to configure Bluetooth device access rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Local activity control** → **Device Control** and click **Settings**.
4. Under **Device Control settings**, select the **Types of devices** tab.

   The table lists access rules for all devices that are present in the classification of the Device Control component.
5. In the context menu for the **Bluetooth** device type, configure the Bluetooth device access mode: **Allow** , **Block** , **Allow and do not log** .

   If you blocked access to Bluetooth devices, you can allow connecting input devices (keyboards, mice, etc) only in the Application Console or in Kaspersky Security Center Web Console. You cannot allow connecting input devices in the Kaspersky Security Center Administration Console.
6. Save your changes.

How to configure Bluetooth device access rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.

4. In the policy window, select **Local activity control** → **Device Control** and click **Settings**.
5. In the **Device Control Settings** block, click the **Access rules for devices and Wi-Fi networks** link.

   The table lists access rules for all devices that are present in the classification of the Device Control component.
6. Select the **Bluetooth** device type.

   This opens the Bluetooth device access settings.
7. Configure the Bluetooth device access mode: **Allow**, **Block**, **Allow and do not log**.
8. If you select the **Block** mode, you can allow connecting only Bluetooth input devices (keyboards, mice, etc). To do so, under **Exclusions**, select the **Input devices (mice and keyboards)** check box.
9. Save your changes.

How to configure Bluetooth device access rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.
3. Under **Device Control settings**, select the **Types of devices** tab.

   The table lists access rules for all devices that are present in the classification of the Device Control component.
4. Under **Access**, configure the Bluetooth device access mode: **Allow**, **Block**, **Allow and do not log**.
5. If you select the **Block** mode, you can allow connecting only Bluetooth input devices (keyboards, mice, etc). To do so, under **Exclusions**, select the **Input devices (mice and keyboards)** check box.
6. Save your changes.

Differentiation of user access rights to devices

You can configure user access rights by device type or to trusted devices.

Differentiation of user access rights by device type

Device Control allows configuring user access rights to data on *storage devices*. For such devices, you can configure write and read permissions. Device Control supports the following types of storage devices:

- Hard drives
- Removable drives
- Floppy disks

- CD/DVD drives
- Portable devices (MTP) Portable devices (MTP) include, for example, mobile devices, photo cameras, media players, and so on.

In this way you can, for example, allow using removable media only to the group of administrators. For other device types, you can deny or allow access for all users. You can also configure user access rights to use printers.

How to configure user access rights to data on removable drives in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Select the **Device Control** check box.
6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.
7. Under **Device Control settings**, select the **Types of devices** tab.

   The **Types of devices** tab shows access rules for all devices that are included in the Device Control classification.
8. To configure storage device access rules, double-click to open the list of rules.
9. Configure the storage device access rule:

   a. In the **Access rules** block, click the **Add** button.

      This opens a window for adding a new storage device access rule.

   b. In the **Priority** field, set the *rule write* priority. A rule includes the following attributes: user account, schedule, permissions (read/write), and priority.

      A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

      For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

      The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

   c. Under **Rule for users and groups**, select users or groups of users. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

   d. Click **OK**.

10. Under **Schedules for the selected access rule**, configure a storage device access schedule for users.

    For example, you can allow users to use storage devices only during working hours.

11. Configure users' access permissions to storage devices in the file manager (**Read** / **Write**).

12. Save your changes. To apply the policy on computers, close the padlocks .

How to configure user access rights to data on storage devices in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.

5. Select the **Enable Device Control** check box.

6. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

7. In the **Device Control Settings** block, click **Access rules for devices and Wi-Fi networks**.

   A window opens with access rules for all devices that are included in the Device Control component classification.

8. In the **Access To Storage Devices** block, open the properties of the storage device access rule.

9. Configure the storage device access rule:

   a. In the **Users** block, click the **Add** button.

      This opens a window for adding a new storage device access rule.

   b. In the **Priority** field, set the *rule write* priority. A rule includes the following attributes: user account, schedule, permissions (read/write), and priority.

      A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

      For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

      The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

   c. Under **Users**, select users or groups of users. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

d. Under **Schedule for access to devices**, configure a storage device access schedule for users.

For example, you can allow users to use storage devices only during working hours.

e. Configure users' access permissions to storage devices in the file manager (**Read** / **Write**).

f. Click **OK**.

10. Save your changes. To apply the policy on computers, close the padlocks.

How to configure user access rights to data on storage devices in the Kaspersky Industrial CyberSecurity for Nodes Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.

2. In the results pane of the **Device Control** node, click **Properties**.

The **Properties: Device Control** window opens.

3. Select the **Device Control** check box.

4. In the **Operating mode for blocking rules** block, select **Block** or **Inform**.

5. Under **Device Control settings**, select the **Types of devices** tab.

A window opens with access rules for all devices that are included in the Device Control component classification.

6. To configure storage device access rules, double-click to open the list of rules.

7. Configure the storage device access rule:

a. In the **Access rules** block, click the **Add** button.

This opens a window for adding a new storage device access rule.

b. In the **Rule priority** field, set the *rule write* priority. A rule includes the following attributes: user account, schedule, permissions (read/write), and priority.

A rule has a specific priority. If a user has been added to multiple groups, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on the rule with the highest priority. Kaspersky Industrial CyberSecurity for Nodes allows you to assign priority from 0 to 10,000. The higher the value, the higher the priority. In other words, an entry with the value of 0 has the lowest priority.

For example, you can grant read-only permissions to the Everyone group and grant read/write permissions to the administrators group. To do so, assign a priority of 1 for the administrators group and assign a priority of 0 for the Everyone group.

The priority of a block rule is higher than the priority of an allow rule. In other words, if a user has been added to multiple groups and the priority of all rules are the same, Kaspersky Industrial CyberSecurity for Nodes regulates device access based on any existing block rule.

c. Under **Rule for users and groups**, select users or groups of users. You can select users in Active Directory or enter a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

d. Click **OK**.

8. Under **Schedules for the selected access rule**, configure a storage device access schedule for users.

For example, you can allow users to use storage devices only during working hours.

9. Configure users' access permissions to storage devices in the file manager (**Read** / **Write**).

10. Save your changes.

Differentiation of user access rights to trusted devices

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times. To work with trusted devices, you can grant access to an individual user, to a group of users, or to all users of the organization. You can configure user access rights in the properties of the trusted device.

About Rule Generator for Device Control

You can generate Device Control rules using Kaspersky Security Center tasks and policies simultaneously for all protected devices and groups of protected devices on the corporate network. To create a list of trusted devices, you must conduct an audit of external devices in your organization.

To create a list of rules based on the list of devices connected to an individual protected device, you can run the *Rule Generator for Device Control* task locally using the Application Console.

You can create Device Control rules using Kaspersky Security Center in the following ways:

- Using the *Rule Generator for Device Control* task.

  Depending on its settings, the *Rule Generator for Device Control* task, can collect information about all devices that have ever been connected to the computer, and for which information is stored in the operating system; or about devices that are connected at the moment when the task is started. Based on the collected information, the task generates a list of allow rules for the Device Control component. You can configure automatic import of generated rules to the list of Device Control component rules, or import the generated rules manually.

  This scenario can be used, for example, if you need to quickly create allow rules for trusted devices that you have used in the past before running the Device Control component for the first time.

  How to run the Rule Generator for Device Control task in the Kaspersky Security Center Administration Console

  1. Open the Kaspersky Security Center Administration Console.

  2. In the console tree, select **Tasks**.

  3. Select the *Rule Generator for Device Control* task and double-click to open the task properties.

     If necessary, create a new task.

  4. In the **Mode** section, select the mode of the task:

     - **Consider system data about all external devices that have ever been connected**.

       The application gets information about all devices that have been connected to the computer from operating system memory.

     - **Consider currently connected external devices only**.

       The application gets information about devices that are connected when the task is started.

5. Enter the path where you want to save the file with data.

6. If you run the task on multiple computers, we recommend selecting the **Add protected device details to the file name** check box.

7. Save your changes.

8. Run the task.

How to run a Rule Generator for Device Control task in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

   The list of tasks opens.

2. Select the *Rule Generator for Device Control* task and double-click to open the task properties.

   If necessary, create a new task.

3. In the **Mode** section, select the mode of the task:

   - **Consider system data about all external devices that have ever been connected**.

     The application gets information about all devices that have been connected to the computer from operating system memory.

   - **Consider currently connected external devices only**.

     The application gets information about devices that are connected when the task is started.

4. Enter the path where you want to save the file with data.

5. If you run the task on multiple computers, we recommend selecting the **Add protected device details to the file name** check box.

6. Save your changes.

7. Run the task.

How to run a Rule Generator for Device Control task in the Web Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Automatic Rule Generation** → **Rule Generator for Device Control**.

2. In the results pane of the **Rule Generator for Device Control** node, click **Properties**.

   The **Properties: Rule Generator for Device Control** window opens.

3. In the **Mode** section, select the mode of the task:

   - **Consider system data about all external devices that have ever been connected**.

     The application gets information about all devices that have been connected to the computer from operating system memory.

   - **Consider currently connected external devices only**.

     The application gets information about devices that are connected when the task is started.

4. In the **After task completes** section, select application actions after the task is completed:

   - **Add allowing rules to the list of Device Control rules**. The list of device control rules is available in the Device Control component settings.

     If this check box is selected, the application adds the rules generated by the task to the list of Device Control rules based on the selected principle for adding rules.

     If this check box is cleared, the application does not add the newly generated allowing rules to the list of Device Control rules. The application only exports rules to a file.

   - **Principle of adding**. A method used to add the newly generated allowing rules to the list of Device Control rules:

     - **Add to existing rules**. The application adds a rule to the list of existing rules. In this case, the application duplicates identical rules.

     - **Replace existing rules**. The application adds new rules instead of existing rules.

     - **Merge with existing rules**. The application adds a rule to the list of existing rules. In this case, the application merges identical rules.

   - **Export allowing rules to file**. The application exports allowing rules to the file specified in the field below. You can then import the file in the application settings on other computers to distribute the allowing rules. The file can also be used to back up the allowing rules.

   - **Add protected device details to the file name**. In addition to the date and time, the application adds the computer name to the exported file name. It is convenient if you collect allowing rules from several computers.

5. Save your changes.

As a result, Kaspersky Industrial CyberSecurity for Nodes conducts an audit of external devices and saves the information in the registry of Kaspersky Security Center. The external device list is available when adding trusted devices.

> The *Rule Generator for Device Control* task does not collect information about network printers and Wi-Fi networks connected to devices. For devices of these types, you need to create rules manually.

- Based on the event report generated in Kaspersky Security Center for the Device Control component, running in **Inform** mode.

  Under this scenario, Kaspersky Industrial CyberSecurity for Nodes does not block access to devices. When the component Device Control runs in the **Inform** mode, the application allows all devices to be used and logs external device connection and disconnection events.

  How to enable Device Control in Inform mode in the Kaspersky Security Center Administration Console

  1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

  2. Select the necessary policy and double-click to open the policy properties.

  3. In the policy properties window, select **Local activity control**.

  4. In the **Device Control** section, click **Settings**.

  5. Select the **Device Control** check box.

6. Under **Operating mode for blocking rules**, select **Inform**.
7. Save your changes. To apply the policy on computers, close the padlocks.

How to enable Device Control in Inform mode in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local activity control** → **Device Control** and click the **Configure** button.
   The **Device Control** window opens.
5. Select the **Enable Device Control** check box.
6. Under **Operating mode for blocking rules**, select **Inform**.
7. Save your changes. To apply the policy on computers, close the padlocks.

How to enable Device Control in Inform mode in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.
   The **Properties: Device Control** window opens.
3. Select the **Device Control** check box.
4. Under **Operating mode for blocking rules**, select **Inform**.
5. Save your changes.

While the component is running, all possible scenarios for protected devices and protected device groups must be executed. Then you can import the information from the Kaspersky Security Center event report to a TXT file and, after reviewing the report, add trusted devices.

This scenario is recommended if a corporate network includes a large number of protected devices of different type with a different set of external devices.

Adding trusted devices

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

To work with trusted devices, you can grant access to an individual user, to a group of users, or to all users of the organization.

For example, if your organization does not allow the use of removable drives but administrators use removable drives in their work, you can allow removable drives only for a group of administrators. To do so, add removable drives to the trusted list and configure user access permissions.

It is not recommended to add more than 1000 trusted devices, as this can cause system instability.

How to add a trusted device in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Under **Devices monitoring settings**, select the **Trusted devices** tab.

   This opens the list of trusted devices.
6. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted devices for all computers in the company.

   The lists of trusted devices in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted devices from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted devices of the parent policy is not possible.
7. Click the **Add** button and select a method for adding a device to the trusted list:

   - **Generate rules based on connected devices**.
   - **Generate rules based on system data**.
   - **Generate rules based on Kaspersky Security Center registry**.

   If the list of devices is empty, you must conduct an audit of external devices. To do so, run the *Rule Generator for Device Control* task.

   Kaspersky Industrial CyberSecurity for Nodes does not support adding devices of the **Floppy disks** type to the trusted list.
8. Click **Add rules for selected devices**.
9. Save your changes. To apply the policy on computers, close the padlocks.

How to add a trusted device in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.

4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.

5. In the **Device Control Settings** block, click **Trusted devices**.

   This opens the list of trusted devices.

6. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted devices for all computers in the company.

   The lists of trusted devices in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted devices from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted devices of the parent policy is not possible.

7. Click **From KSC registry**.

   If the list of devices is empty, you must conduct an audit of external devices. To do so, run the *Rule Generator for Device Control* task.

   > Kaspersky Industrial CyberSecurity for Nodes does not support adding devices of the **Floppy disks** type to the trusted list.

8. Save your changes. To apply the policy on computers, close the padlocks.

How to add a trusted device in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.

2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.

3. Under **Device Control settings**, select the **Trusted devices** tab.

   This opens the list of trusted devices.

4. Click the **Add** button and select a method for adding a device to the trusted list:

   - **Generate rules based on connected devices**.
   - **Generate rules based on system data**.
   - **Generate rules based on Kaspersky Security Center registry**.

   If the list of devices is empty, you must conduct an audit of external devices. To do so, run the *Rule Generator for Device Control* task.

   > Kaspersky Industrial CyberSecurity for Nodes does not support adding devices of the **Floppy disks** type to the trusted list.

5. Click **Add rules for selected devices**.

6. Save your changes.

Exporting and importing the list of trusted devices

To distribute the list of trusted devices to other computers in your organization, you can use the export/import procedure. You can export the list of trusted devices to an XML file. Then you can modify the file to, for example, add a large number of devices of the same type. You can use the export/import function to back up the list of trusted devices or to migrate the list to a different server.

Kaspersky Industrial CyberSecurity for Nodes allows importing the list of trusted devices from Kaspersky Endpoint Security for Windows. The XML file format for these applications is the same.

How to export and import a list of trusted devices in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Local activity control**.
4. In the **Device Control** section, click **Settings**.
5. Under **Device Control settings**, select the **Trusted devices** tab.

   This opens the list of trusted devices.
6. To export the list of trusted devices:

   a. If you want to export the entire list, click the button and select **Export**.

   b. If you want to export only part of the list, follow these steps:

      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.
      2. Click the button and select **Export selected**.

   c. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of trusted devices to the XML file.
7. To import the list of trusted devices:

   a. Click **Add** → **Import rules from XML file** and select an import mode: add or replace.

      In the window that opens, select the XML file from which you want to import the list of trusted devices.

      In merge mode, the application checks the lists of trusted devices and removes duplicate entries. In add mode, the application adds entries to the trusted application list without checking for duplicates.

   b. Open the file.

      Kaspersky Industrial CyberSecurity for Nodes imports trusted devices according to the selected mode.
8. Save your changes. To apply the policy on computers, close the padlocks .

How to export and import a list of trusted devices in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local activity control** → **Device Control** and click the **Configure** button.

   The **Device Control** window opens.
5. In the **Device Control Settings** block, click **Trusted devices**.

   This opens the list of trusted devices.
6. To export the list of trusted devices:

   a. Select the trusted devices that you want to export.

   b. Click the **Export** button and select the export mode: export the whole list of trusted devices or only selected trusted devices.

   c. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the list of web resource addresses to a XML file.
7. To import the list of trusted devices:

   a. Click the **Import** button and select an import mode: add or replace.

   b. In the window that opens, select the XML file from which you want to import the list of web resources.

   c. Open the file.

   Kaspersky Industrial CyberSecurity for Nodes imports trusted devices according to the selected mode.
8. Save your changes. To apply the policy on computers, close the padlocks .

How to export and import a list of trusted devices in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Device Control**.
2. In the results pane of the **Device Control** node, click **Properties**.

   The **Properties: Device Control** window opens.
3. Under **Device Control settings**, select the **Trusted devices** tab.

   This opens the list of trusted devices.

4. To export the list of trusted devices:

   a. If you want to export the entire list, click the button and select **Export**.

   b. If you want to export only part of the list, follow these steps:

      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

      2. Click the button and select **Export selected**.

   c. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of trusted devices to the XML file.

5. To import the list of trusted devices:

   a. Click **Add** → **Import rules from XML file** and select an import mode: add or replace.

      In the window that opens, select the XML file from which you want to import the list of web resources.

      In merge mode, the application checks the lists of trusted devices and removes duplicate entries. In add mode, the application adds entries to the trusted application list without checking for duplicates.

   b. Open the file.

      Kaspersky Industrial CyberSecurity for Nodes imports trusted devices according to the selected mode.

6. Save your changes.

Firewall

The Firewall component can work in the following modes:

- **Observe the state of Windows Firewall**. The mode is intended for smooth transition from the logic of the Firewall Management task in the application version 4.0 and below to the full-featured Firewall in the application version 4.5 and later. When you upgrade the application version 4.0 and below, the rules of the Firewall Management task integrated into the Windows Firewall are retained. But the Firewall component no longer interacts with Windows Firewall, but only monitors Windows Firewall traffic filtering and records the corresponding events in the component's operation log. You can then create Firewall rules and/or import Windows Firewall rules and change the Firewall operating mode to **Inform**.

- **Inform**. The application only monitors the operation of the Firewall rules and records the corresponding events in the component's operation log. The mode is intended for testing the Firewall rules. You can evaluate their applicability using the Firewall operation log. Then, if necessary, you can adjust the Firewall rules and change the Firewall operation mode to **Block**.

- **Block**. The application filters network traffic in accordance with the component settings and records the corresponding events in the component's operation log.

About Firewall rules

If the **Block** mode is selected, the Firewall component filters network traffic using Firewall rules.

Firewall rules for applications control network connections for specified applications. The triggering criterion for these rules is based on the path to an executable application file.

Firewall port rules control network connections for specified ports and protocols (TCP / UDP). The triggering criteria for such rules are protocol type and port or port range.

> Port rules involve a broader scope than application rules. By allowing network connections based on port rules, you lower the security level of the protected computer.

Configuring the Firewall

This section provides instructions on configuring general settings of the Firewall component and creating and configuring Firewall rules.

Configuring general Firewall settings

Configuring general settings of the Firewall component in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the **Network activity control** section, click the **Settings** button in the **Firewall** subsection.

   The **Firewall** window opens.
4. On the **General** tab in the **Operating mode for blocking rules** block, select the component operating mode:

   - **Observe the state of Windows Firewall**. The mode is intended for smooth transition from the logic of the Firewall Management task in the application version 4.0 and below to the full-featured Firewall in the application version 4.5 and later. When you upgrade the application version 4.0 and below, the rules of the Firewall Management task integrated into the Windows Firewall are retained. But the Firewall component no longer interacts with Windows Firewall, but only monitors Windows Firewall traffic filtering and records the corresponding events in the component's operation log. You can then create Firewall rules and/or import Windows Firewall rules and change the Firewall operating mode to **Inform**.
   - **Inform**. The application only monitors the operation of the Firewall rules and records the corresponding events in the component's operation log. The mode is intended for testing the Firewall rules. You can evaluate their applicability using the Firewall operation log. Then, if necessary, you can adjust the Firewall rules and change the Firewall operation mode to **Block**.
   - **Block**. The application filters network traffic in accordance with the component settings and records the corresponding events in the component's operation log.
5. In the **Inbound connections** block, configure the settings for incoming network connections:

   - Use the **Action for inbound connections** drop-down list to specify the action that the application performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.
   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, the application allows incoming network connections that match the rule criteria.

6. In the **Outbound connections** block, configure the settings for outgoing network connections:

   - Use the **Action for outbound connections** drop-down list to specify the action that the application performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.

   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, the application blocks outgoing network connections that match the rule criteria.

7. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Configuring general settings of the Firewall component in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. In the **Network activity control** section, click the **Configure** button in the **Firewall** subsection.

   The **Firewall** window opens.

5. Set the toggle switch to **Firewall ENABLED**.

6. In the **Operating mode for blocking rules** block, select the component operating mode:

   - **Observe the state of Windows Firewall**. The mode is intended for smooth transition from the logic of the Firewall Management task in the application version 4.0 and below to the full-featured Firewall in the application version 4.5 and later. When you upgrade the application version 4.0 and below, the rules of the Firewall Management task integrated into the Windows Firewall are retained. But the Firewall component no longer interacts with Windows Firewall, but only monitors Windows Firewall traffic filtering and records the corresponding events in the component's operation log. You can then create Firewall rules and/or import Windows Firewall rules and change the Firewall operating mode to **Inform**.

   - **Inform**. The application only monitors the operation of the Firewall rules and records the corresponding events in the component's operation log. The mode is intended for testing the Firewall rules. You can evaluate their applicability using the Firewall operation log. Then, if necessary, you can adjust the Firewall rules and change the Firewall operation mode to **Block**.

   - **Block**. The application filters network traffic in accordance with the component settings and records the corresponding events in the component's operation log.

7. In the **Inbound connections** block, configure the settings for incoming network connections:

   - Use the **Action for inbound connections** drop-down list to specify the action that the application performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.

   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, the application allows incoming network connections that match the rule criteria.

8. In the **Outbound connections** block, configure the settings for outgoing network connections:

   - Use the **Action for outbound connections** drop-down list to specify the action that the application performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.

   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, the application blocks outgoing network connections that match the rule criteria.

9. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Configuring general settings of the Firewall component in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Firewall**.

2. In the results pane of the **Firewall** node, click **Properties**.

   The **Properties: Firewall** window opens.

3. Select the **Firewall** check box.

4. In the **Operating mode for blocking rules** block, select the component operating mode:

   - **Observe the state of Windows Firewall**. The mode is intended for smooth transition from the logic of the Firewall Management task in the application version 4.0 and below to the full-featured Firewall in the application version 4.5 and later. When you upgrade the application version 4.0 and below, the rules of the Firewall Management task integrated into the Windows Firewall are retained. But the Firewall component no longer interacts with Windows Firewall, but only monitors Windows Firewall traffic filtering and records the corresponding events in the component's operation log. You can then create Firewall rules and/or import Windows Firewall rules and change the Firewall operating mode to **Inform**.

   - **Inform**. The application only monitors the operation of the Firewall rules and records the corresponding events in the component's operation log. The mode is intended for testing the Firewall rules. You can evaluate their applicability using the Firewall operation log. Then, if necessary, you can adjust the Firewall rules and change the Firewall operation mode to **Block**.

   - **Block**. The application filters network traffic in accordance with the component settings and records the corresponding events in the component's operation log.

5. In the **Inbound connections** block, configure the settings for incoming network connections:

   - Use the **Action for inbound connections** drop-down list to specify the action that the application performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.

   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, the application allows incoming network connections that match the rule criteria.

6. In the **Outbound connections** block, configure the settings for outgoing network connections:

   - Use the **Action for outbound connections** drop-down list to specify the action that the application performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.

   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, the application blocks outgoing network connections that match the rule criteria.

7. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Creating and configuring Firewall rules

Creating and configuring Firewall rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the **Network activity control** section, click the **Settings** button in the **Firewall** subsection.

   The **Firewall** window opens.

4. In the **Inbound connections** block, click the **Rules list** button.

   The **Rules for inbound connections** window opens.

5. **Create and configure Firewall rules for incoming connections**.

   1. On the **Applications** tab, click the **Add** button.

      The **Rule for an application** window opens.

2. Configure the rule settings:

   a. In the **Rule name** field, enter the name of the rule.

      The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections.

   b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the application.
      - **Block**. If this option is selected, the application blocks incoming network connections for the application.

   c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

   d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

   e. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

   f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

   g. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

      Only the IPv4 format is supported for IP addresses.

   h. In the **Network adapters** block, specify the list of network adapters.

   i. Click the **OK** button to save the rule.

3. On the **Ports** tab, click the **Add** button.

   The **Rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field, enter the name of the rule.

   b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the ports.
      - **Block**. If this option is selected, the application blocks incoming network connections for the ports.

   c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

   d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

e. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

> Only the IPv4 format is supported for IP addresses.

f. In the **Network adapters** block, specify the list of network adapters.

g. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for inbound connections** window.

6. In the **Outbound connections** block, click the **Rules list** button.

   The **Rules for outbound connections** window opens.

7. **Create and configure Firewall rules for outgoing connections**.

   1. On the **Applications** tab, click the **Add** button.

      The **Rule for an application** window opens.

   2. Configure the rule settings:

      a. In the **Rule name** field, enter the name of the rule.

      > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections.

      b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows outgoing network connections for the application.
      - **Block**. If this option is selected, the application blocks outgoing network connections for the application.

      c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

      d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

      e. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

      f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

      g. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

      > Only the IPv4 format is supported for IP addresses.

h. In the **Network adapters** block, specify the list of network adapters.

i. Click the **OK** button to save the rule.

3. On the **Ports** tab, click the **Add** button.

   The **Rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field, enter the name of the rule.

   b. In the **Action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the ports.

   c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

   d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

   e. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

   > Only the IPv4 format is supported for IP addresses.

   f. In the **Network adapters** block, specify the list of network adapters.

   g. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for outbound connections** window.

8. If you want to import or export custom rules from an XML file, use the **Import** or **Export** buttons in the **Import and export of rules** block.

9. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Creating and configuring Firewall rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. In the **Network activity control** section, click the **Configure** button in the **Firewall** subsection.

   The **Firewall** window opens.

5. Set the toggle switch to **Firewall ENABLED**.

6. In the **Inbound connections** block, click the **Configure** button.

   The **Rules for inbound connections** window opens.

7. **Create and configure Firewall rules for incoming connections**.

   1. On the **Ports** tab, click the **Add** button.

      The **Rule for ports** window opens.

   2. Configure the rule settings:

      a. In the **Rule name** field, enter the name of the rule.

      b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the ports.
      - **Deny**. If this option is selected, the application blocks incoming network connections for the ports.

      c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

      d. In the **Local ports** and **Remote ports** blocks, specify a port or range of ports.

      e. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections to the specified network addresses in accordance with the rule settings.

      > Only the IPv4 format is supported for IP addresses.

      f. In the **Network adapters** block, specify the list of network adapters.

      g. Click the **OK** button to save the rule.

   3. On the **Applications** tab, click the **Add** button.

      The **Rule for applications** window opens.

   4. Configure the rule settings:

      a. In the **Rule name** field, enter the name of the rule.

      > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections.

      b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the application.
      - **Deny**. If this option is selected, the application blocks incoming network connections for the application.

c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

d. In the **Local ports** and **Remote ports** blocks, specify a port or range of ports.

e. In the **Application path** field, manually specify the path to the executable file of the application for which you are configuring the rule.

f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

g. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

> Only the IPv4 format is supported for IP addresses.

h. In the **Network adapters** block, specify the list of network adapters.

i. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for inbound connections** window.

8. In the **Outbound connections** block, click the **Configure** button.

   The **Rules for outbound connections** window opens.

9. **Create and configure Firewall rules for outgoing connections**.

   1. On the **Ports** tab, click the **Add** button.

      The **Rule for ports** window opens.

   2. Configure the rule settings:

      a. In the **Rule name** field, enter the name of the rule.

      b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
      - **Deny**. If this option is selected, the application blocks outgoing network connections for the ports.

      c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

      d. In the **Local ports** and **Remote ports** blocks, specify a port or range of ports.

      e. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

      > Only the IPv4 format is supported for IP addresses.

      f. In the **Network adapters** block, specify the list of network adapters.

      g. Click the **OK** button to save the rule.

3. On the **Applications** tab, click the **Add** button.

   The **Rule for applications** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field, enter the name of the rule.

   > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections.

   b. In the **Action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the application.
   - **Deny**. If this option is selected, the application blocks outgoing network connections for the application.

   c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

   d. In the **Local ports** and **Remote ports** blocks, specify a port or range of ports.

   e. In the **Application path** field, manually specify the path to the executable file of the application for which you are configuring the rule.

   f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

   g. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

   > Only the IPv4 format is supported for IP addresses.

   h. In the **Network adapters** block, specify the list of network adapters.

   i. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for outbound connections** window.

10. If you want to import or export custom rules from an XML file, use the **Import of rules** or **Export of rules** buttons in the **Import and export of rules** block.

11. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Creating and configuring Firewall rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Firewall**.
2. In the results pane of the **Firewall** node, click **Properties**.

   The **Properties: Firewall** window opens.
3. In the **Inbound connections** block, click the **Rules list** button.

   The **Rules for inbound connections** window opens.
4. **Create and configure Firewall rules for incoming connections**.

   1. On the **Applications** tab, click the **Add** button.

      The **Rule for an application** window opens.
   2. Configure the rule settings:

      a. In the **Rule name** field, enter the name of the rule.

      > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections.

      b. In the **Action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the application.
      - **Block**. If this option is selected, the application blocks incoming network connections for the application.

      c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

      d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

      e. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

      f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

      g. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

      > Only the IPv4 format is supported for IP addresses.

      h. In the **Network adapters** block, specify the list of network adapters.

      i. Click the **OK** button to save the rule.
   3. On the **Ports** tab, click the **Add** button.

      The **Rule for ports** window opens.

4. Configure the rule settings:

    a. In the **Rule name** field, enter the name of the rule.

    b. In the **Action** list, select one of the options:

    - **Allow**. If this option is selected, the application allows incoming network connections for the ports.
    - **Block**. If this option is selected, the application blocks incoming network connections for the ports.

    c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

    d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

    e. In the **Rule usage scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

    > Only the IPv4 format is supported for IP addresses.

    f. In the **Network adapters** block, specify the list of network adapters.

    g. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for inbound connections** window.

5. In the **Outbound connections** block, click the **Rules list** button.

   The **Rules for outbound connections** window opens.

6. **Create and configure Firewall rules for outgoing connections**.

    1. On the **Applications** tab, click the **Add** button.

       The **Rule for an application** window opens.

    2. Configure the rule settings:

        a. In the **Rule name** field, enter the name of the rule.

        > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections.

        b. In the **Action** list, select one of the options:

        - **Allow**. If this option is selected, the application allows outgoing network connections for the application.
        - **Block**. If this option is selected, the application blocks outgoing network connections for the application.

        c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

e. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

f. In the **Service name** field, if necessary, specify the name of the service for which the rule will be applied.

g. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

> Only the IPv4 format is supported for IP addresses.

h. In the **Network adapters** block, specify the list of network adapters.

i. Click the **OK** button to save the rule.

3. On the **Ports** tab, click the **Add** button.

   The **Rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field, enter the name of the rule.

   b. In the **Action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the ports.

   c. Select the **Protocol** check box, to select the protocol type for which the application controls incoming network connections.

   d. In the **Ports** and **Ports** blocks, specify a port or range of ports.

   e. In the **Rule usage scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

   > Only the IPv4 format is supported for IP addresses.

   f. In the **Network adapters** block, specify the list of network adapters.

   g. Click the **OK** button to save the rule.

5. Click the **OK** button in the **Rules for outbound connections** window.

7. If you want to import or export custom rules from an XML file, use the **Import** or **Export** buttons in the **Import and export of rules** block.

8. To import Windows Firewall rules, click **Import Windows Firewall rules**.

   On Windows 11 24H2 computers, the application may skip certain Windows Firewall rules. Because of special features of this version of the operating system, Kaspersky Industrial CyberSecurity for Nodes may not recognize the parameters of some rules for application packets.

9. Save your changes.

Kaspersky Industrial CyberSecurity for Nodes applies the new settings. The date and time when the settings were changed are saved in the system audit log.

Enabling and disabling Firewall rules

Enabling and disabling Firewall rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the **Network activity control** section, click the **Settings** button in the **Firewall** subsection.

   The **Firewall** window opens.
4. In the window that opens, click the **Rules list** button in the **Inbound connections** or **Outbound connections** section, depending on the type of rule whose status you want to change.
5. In the window that opens, select the **Applications** or **Ports** tab.

   In the rule list, select the rule whose status you want to modify and perform one of the following actions:

   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.
   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.
6. To delete rules from the list, select the rules and click **Delete**.
7. Save your changes.

Enabling and disabling Firewall rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. In the **Network activity control** section, click the **Configure** button in the **Firewall** subsection.

   The **Firewall** window opens.

5. In the window that opens, click the **Configure** button in the **Inbound connections** or **Outbound connections** section, depending on the type of rule whose status you want to change.

6. In the window that opens, select the **Ports** or **Applications** tab.

   In the rule list, select the rule whose status you want to modify and perform one of the following actions:

   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.

   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.

7. To delete rules from the list, select the rules and click **Delete**.

8. Save your changes.

Enabling and disabling Firewall rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Computer Control** → **Firewall**.

2. In the results pane of the **Firewall** node, click **Properties**.

   The **Properties: Firewall** window opens.

3. In the window that opens, click the **Rules list** button in the **Inbound connections** or **Outbound connections** section, depending on the type of rule whose status you want to change.

4. In the window that opens, select the **Applications** or **Ports** tab.

   In the rule list, select the rule whose status you want to modify and perform one of the following actions:

   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.

   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.

5. To delete rules from the list, select the rules and click **Delete**.

6. Save your changes.

BadUSB Attack Prevention

The BadUSB Attack Prevention component is not installed by default. You can add a component during application installation or change the set of application components after the application is installed.

Some viruses modify the firmware of USB devices to trick the operating system into detecting the USB device as a keyboard. As a result, the virus may execute commands under your user account to download malware, for example.

The BadUSB Attack Prevention component prevents infected USB devices emulating a keyboard from connecting to the computer.

When a USB device is connected to the computer and identified as a keyboard by the operating system, the application prompts the user to enter a numerical code generated by the application from this keyboard or using On-Screen Keyboard if available. This procedure is known as keyboard authorization.

If the code has been entered correctly, the application saves the identification parameters—VID/PID of the keyboard and the number of the port to which it has been connected—in the list of authorized keyboards. Keyboard authorization does not need to be repeated when the keyboard is reconnected or after the operating system is restarted.

When the authorized keyboard is connected to a different USB port of the computer, the application shows a prompt for re-authorization of this keyboard.

If the numerical code has been entered incorrectly, the application generates a new code. You can configure the number of attempts for entering the numerical code. If the numerical code is entered incorrectly several times or the keyboard authorization window is closed, the application blocks input from this keyboard. When the USB device blocking time elapses or the operating system is restarted, the application prompts the user to perform keyboard authorization again.

The application allows use of an authorized keyboard and blocks a keyboard that has not been authorized.

USB devices identified by the operating system as keyboards and connected to the computer before installation of the BadUSB Attack Prevention component are considered authorized after installation of the component.

How to enable and configure the BadUSB Attack Prevention component in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Local activity control** section.
4. In the **BadUSB Attack Prevention** block, click the **Settings** button.

   The **BadUSB Attack Prevention** window opens.
5. Use the **BadUSB Attack Prevention** check box to enable or disable the component.

6. In the **Authorization of USB devices** section, configure the following settings:

   - **Maximum number of USB device authorization attempts**. Automatically blocking the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Industrial CyberSecurity for Nodes displays the blocking duration for the USB device. After this time elapses, you can have five attempts to enter the authorization code.

   - **Timeout when reaching the maximum number of attempts (minutes)**. Blocking duration of the USB device after the specified number of failed attempts to enter the authorization code. Valid values are 1 to 180 (minutes).

7. In the **USB device authorization upon connection** section, configure the following settings:

   - **Prohibit use of On-Screen Keyboard for authorization of USB devices**. If the check box is selected, the application blocks use of On-Screen Keyboard for authorization of USB devices from which an authorization code cannot be entered (e.g. barcode scanners).

   - **Prohibit use of a barcode for authorization of USB devices**. If the check box is selected, the application does not show the barcode in the barcode scanner authorization notification.

8. Close the padlocks to apply the policy to computers.

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

How to enable and configure the BadUSB Attack Prevention component in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Local activity control** section.

5. In the **BadUSB Attack Prevention** block, click the **Configure** button.

   The **BadUSB Attack Prevention** window opens.

6. Use the **BadUSB Attack Prevention** toggle to enable or disable the component.

7. Enable or disable the **Prohibit use of On-Screen Keyboard for authorization of USB devices ENABLED** toggle switch to allow or block the use of On-Screen Keyboard for authorization of USB devices from which an authorization code cannot be entered (e.g. barcode scanners).

8. Enable or disable the **Prohibit use of a barcode for authorization of USB devices ENABLED** toggle switch to allow or block the display of a barcode in the notification for barcode scanner authorization.

9. In the **Authorization of USB devices** section, configure the following settings:

   - **Maximum number of USB device authorization attempts (1-10)**. Automatically blocking the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Industrial CyberSecurity for Nodes displays the blocking duration for the USB device. After this time elapses, you can have five attempts to enter the authorization code.

   - **Timeout when reaching the maximum number of attempts in minutes (1-180)**. Blocking duration of the USB device after the specified number of failed attempts to enter the authorization code. Valid values are 1 to 180 (minutes).

10. Close the padlocks to apply the policy to computers.

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

How to enable and configure the BadUSB Attack Prevention component in the Application Console

1. In the Application Console tree, select the **Computer Control → BadUSB Attack Prevention** section.

2. Click the **Properties** link in the results pane.

   The **BadUSB Attack Prevention** window opens.

3. Use the **BadUSB Attack Prevention** check box to enable or disable the component.

4. In the **Authorization of USB devices** section, configure the following settings:

   - **Maximum number of USB device authorization attempts**. Automatically blocking the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Industrial CyberSecurity for Nodes displays the blocking duration for the USB device. After this time elapses, you can have five attempts to enter the authorization code.

   - **Timeout when reaching the maximum number of attempts (minutes)**. Blocking duration of the USB device after the specified number of failed attempts to enter the authorization code. Valid values are 1 to 180 (minutes).

5. In the **USB device authorization upon connection** section, configure the following settings:

   - **Prohibit use of On-Screen Keyboard for authorization of USB devices**. If the check box is selected, the application blocks use of On-Screen Keyboard for authorization of USB devices from which an authorization code cannot be entered (e.g. barcode scanners).

   - **Prohibit use of a barcode for authorization of USB devices**. If the check box is selected, the application does not show the barcode in the barcode scanner authorization notification.

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

System Integrity Monitoring

Kaspersky Industrial CyberSecurity for Nodes 4.5 now includes the System Integrity Monitoring component instead of the separate File Integrity Monitor and Registry Access Monitor components. System Integrity Monitoring includes all functionality of File Integrity Monitor and additionally allows monitoring registry changes and connection of external devices.

System Integrity Monitoring monitors changes in the operating system that may indicate computer security breaches. When such changes are detected, Kaspersky Industrial CyberSecurity for Nodes generates corresponding events and alerts the administrator. System Integrity Monitoring can operate in real-time mode and can also perform system integrity checks on demand.

Real-Time System Integrity Monitoring

In real-time mode, the System Integrity Monitoring component tracks changes in objects that you included in the component's scope (the monitoring scope). System Integrity Monitoring also allows blocking unauthorized access to such objects in real time.

On-Demand System Integrity Check

On-Demand System Integrity Check is a task that you can run manually or on a schedule. To run the *Baseline System Integrity Monitor* task, you must configure the scope of the component (the monitoring scope) and create a baseline. A baseline is a recorded state of objects in the system, which the application uses as reference when comparing to the current state. A baseline is created when the task is first started.

Migrating File Integrity Monitor settings

When you update Kaspersky Industrial CyberSecurity for Nodes version 4.0 or earlier to version 5.0, File Integrity Monitor and Registry access monitoring settings are migrated automatically. As part of the migration, the application moves the monitoring rules to System Integrity Monitoring.

About System Integrity Monitoring rules

For System Integrity Monitoring to work, you must add at least one rule. A *System Integrity Monitoring rule* is a set of criteria that define the access of users to files or the registry. System Integrity Monitoring detects changes in the files or the registry within the specified *monitoring scope*. The monitoring scope is one of the criteria of a System Integrity Monitoring rule.

System Integrity Monitoring allows monitoring the following objects:

- Files
- Registry
- External devices

Special considerations involved in file monitoring

System Integrity Monitoring monitors changes in files and folders as well as files being added to the monitoring scope or removed from it. These changes may indicate a computer security breach. We recommend adding rarely modified objects or objects that only the administrator has access to. This helps reduce the number of System Integrity Monitoring events.

Kaspersky Industrial CyberSecurity for Nodes monitors the changes of files and folders only on those disks that were connected when Real-Time System Integrity Monitoring began operating. If a disk was not connected when Real-Time System Integrity Monitoring began operating, the application does not monitor the changes of files and folders on that disk even if the files and folders are added to the monitoring scope.

The application generates the Object creation event when one of the following actions is recorded: creating a file, increasing file size, rewriting file data, or truncating a file. Accordingly, if the Object creation event is generated for a file during Applications Launch Control blocking rules operation, this may result from either prohibited file creation or prohibited file modification, including operations such as increasing file size, rewriting data, and truncating.

Special considerations involved in registry monitoring

System Integrity Monitoring monitors the registry. These changes may indicate a computer security breach.

System Integrity Monitoring monitors the following root keys of the registry:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`

- HKEY_USERS
- HKEY_CURRENT_CONFIG

System Integrity Monitoring does not support the HKEY_CURRENT_USER key. You can specify a key under HKEY_USERS as HKEY_USERS\<user profile ID>\<key>.

Special considerations involved in external device monitoring

System Integrity Monitoring monitors connection and disconnection of external devices. This is necessary to protect the computer from security threats that can result from file exchange with such devices. System Integrity Monitoring does not monitor access to external devices and does not block file exchange. You can configure access to devices using a different application component, Device Control.

When running the *Baseline System Integrity Monitor* task, the application ignores the reconnection of external devices if the devices have the same drive letter in the operating system. To be logged, the reconnected devices must have different drive letters.

System Integrity Monitoring monitors the connection of the following types of external devices:

- Removable drive (including USB flash drives)
- Hard drive
- External network adapter
- CD/DVD/Blu-ray drive
- Scanner / camera

Real-Time System Integrity Monitoring

System Integrity Monitoring allows tracking changes in the operating system in real time. You can track changes that may indicate security breaches on the computer. The component allows blocking these changes or merely logging change events.

For System Integrity Monitoring to work, you must add at least one rule. A System Integrity Monitoring rule is a set of criteria that define the access of users to files and the registry. System Integrity Monitoring detects changes in the files and the registry within the specified monitoring scope. The monitoring scope is one of the criteria of a System Integrity Monitoring rule.

How to enable and configure Real-Time System Integrity Monitoring in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, select **System Inspection**.

4. In the **System Integrity Monitoring** section, click **Settings**.

5. Select the **System Integrity Monitoring** check box.

6. Configure the File Integrity Monitor:

   a. Select the **Monitor files** check box on the **Files** tab.

   b. Under **Operating mode for blocking rules**, select a File Integrity Monitor mode:

      - **Block**. In this mode, the application performs actions on files in accordance with File Integrity Monitor rules and generates corresponding events in the System Integrity Monitoring log.

      - **Inform**. In this mode, the application only generates events about triggered File Integrity Monitor rules in the System Integrity Monitoring log.

   c. Add File Integrity Monitor rules manually using the **Add** button or by importing them from an XML file. File Integrity Monitor rule settings are described in the following table.

   d. In the list of File Integrity Monitor rules, manage check boxes to leave the rules that you need enabled.

7. Configure the Registry Access Monitor:

   a. Select the **Monitor the registry** check box on the **Registry** tab.

   b. Under **Operating mode for blocking rules**, select a mode for Registry Access Monitor:

      - **Block**. In this mode, the application blocks actions with the registry in accordance with Registry Access Monitor rules and generates corresponding events in the System Integrity Monitoring log.

      - **Inform**. In this mode, the application only generates events about triggered Registry Access Monitor rules in the System Integrity Monitoring log.

   c. Add Registry Access Monitor rules manually using the **Add** button or by importing them from an XML file. Registry Access Monitor rule settings are described in the following table.

   d. In the list of Registry Access Monitor rules, manage check boxes to leave the rules that you need enabled.

8. Configure external device monitoring:

   a. Select the **Monitor devices** check box on the **Devices** tab.

   b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

      After applying the external device monitoring settings, the application remembers the current external device connections. Subsequently, when an external device is connected or disconnected, the application generates a corresponding event in the System Integrity Monitor log.

9. Save your changes.

How to enable and configure Real-Time System Integrity Monitoring in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **System Inspection** → **System Integrity Monitoring** and click the **Configure** button.
5. Select the **System Integrity Monitoring** check box.
6. Configure the File Integrity Monitor:
   a. Select the **Monitor files** check box on the **Files** tab.
   b. Under **Operating mode for blocking rules**, select a File Integrity Monitor mode:
      - **Block**. In this mode, the application performs actions on files in accordance with File Integrity Monitor rules and generates corresponding events in the System Integrity Monitoring log.
      - **Inform**. In this mode, the application only generates events about triggered File Integrity Monitor rules in the System Integrity Monitoring log.
   c. Add File Integrity Monitor rules manually using the **Add** button or by importing them from an XML file. File Integrity Monitor rule settings are described in the following table.
   d. In the list of File Integrity Monitor rules, manage check boxes in the **Status** column to leave the rules that you need enabled.
7. Configure the Registry Access Monitor:
   a. Select the **Monitor the registry** check box on the **Registry** tab.
   b. Under **Operating mode for blocking rules**, select a mode for Registry Access Monitor:
      - **Block**. In this mode, the application blocks actions with the registry in accordance with Registry Access Monitor rules and generates corresponding events in the System Integrity Monitoring log.
      - **Inform**. In this mode, the application only generates events about triggered Registry Access Monitor rules in the System Integrity Monitoring log.
   c. Add Registry Access Monitor rules manually using the **Add** button or by importing them from an XML file. Registry Access Monitor rule settings are described in the following table.
   d. In the list of Registry Access Monitor rules, manage check boxes in the **Status** column to leave the rules that you need enabled.

8. Configure external device monitoring:

    a. Select the **Monitor devices** check box on the **Devices** tab.

    b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

    System Integrity Monitoring records the current connection of external devices. The application begins to monitor connection and disconnection of external devices after the component is enabled in the application settings. Subsequently, when an external device is connected or disconnected, the application generates a corresponding event.

9. Save your changes.

How to enable and configure Real-Time System Integrity Monitoring in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection → System Integrity Monitoring**.

2. In the results pane of the **System Integrity Monitoring** node, click **Properties**.

    The **Properties: System Integrity Monitoring** window opens.

3. Select the **System Integrity Monitoring** check box.

4. Configure the File Integrity Monitor:

    a. Select the **Monitor files** check box on the **Files** tab.

    b. Under **Operating mode for blocking rules**, select a File Integrity Monitor mode:

    - **Block**. In this mode, the application performs actions on files in accordance with File Integrity Monitor rules and generates corresponding events in the System Integrity Monitoring log.

    - **Inform**. In this mode, the application only generates events about triggered File Integrity Monitor rules in the System Integrity Monitoring log.

    c. Add File Integrity Monitor rules manually using the **Add** button or by importing them from an XML file. File Integrity Monitor rule settings are described in the following table.

    d. In the list of File Integrity Monitor rules, manage check boxes to leave the rules that you need enabled.

5. Configure the Registry Access Monitor:

    a. Select the **Monitor the registry** check box on the **Registry** tab.

    b. Under **Operating mode for blocking rules**, select a mode for Registry Access Monitor:

    - **Block**. In this mode, the application blocks actions with the registry in accordance with Registry Access Monitor rules and generates corresponding events in the System Integrity Monitoring log.

    - **Inform**. In this mode, the application only generates events about triggered Registry Access Monitor rules in the System Integrity Monitoring log.

c. Add Registry Access Monitor rules manually using the **Add** button or by importing them from an XML file. Registry Access Monitor rule settings are described in the following table.

d. In the list of Registry Access Monitor rules, manage check boxes to leave the rules that you need enabled.

6. Configure external device monitoring:

a. Select the **Monitor devices** check box on the **Devices** tab.

b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

After applying the external device monitoring settings, the application remembers the current external device connections. Subsequently, when an external device is connected or disconnected, the application generates a corresponding event in the System Integrity Monitor log.

7. Save your changes.

System Integrity Monitoring rules settings

Parameter	Description
Monitor file operations for the scope	The scope to which you want to apply File Integrity Monitoring. This field is mandatory. Use masks: Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders. Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask. The `?` (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.
Monitored objects	Here you can specify the name or value of a registry key. Use masks: Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a mask:
Operations with files	• **Detect**. The application allows actions on files in the monitoring scope. • **Detect and block**. What the application does depends on the selected File Integrity Monitor mode. If you selected the *Block* mode, System Integrity Monitoring blocks actions with files from the monitoring scope. If you selected the *Inform* mode, System Integrity Monitoring allows actions with files from the monitoring scope.
Trusted users and / or user groups	A trusted user is a user that is allowed to perform actions with files and registry keys in the monitoring scope. If Kaspersky Industrial CyberSecurity for Nodes detects an action performed by a trusted user, System Integrity Monitoring generates an Informational event. You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually.
File operation markers / Actions	Markers characterizing the action with files or registry keys that the application will monitor.
Detect file operations based on all recognized markers / Detect registry operations based on all recognized markers	By default, Kaspersky Industrial CyberSecurity for Nodes detects all file / registry operation markers.
Detect file operations based on the following markers / Detect registry operations based on the following markers	In the list of available file / registry operations select the check boxes next to the operations you want to monitor.

Parameter	Description
Calculate a checksum after a file operation, if possible. The checksum will be indicated in the task log	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes calculates the checksum of the modified file, if a file operation with at least one selected marker was detected. If the file operation is detected by several markers, only the checksum of the final file after all modifications is calculated. If the check box is cleared, Kaspersky Industrial CyberSecurity for Nodes does not calculate the checksum of modified files. No checksum calculation is performed in the following cases: • If the file has become unavailable (for example, due to a change of access permissions). • If the file operation was detected in a file that was subsequently removed. By default, the check box is cleared.
Checksum computing algorithm	Select one of the checksum calculation algorithms from the drop-down list: • MD5 hash • SHA256 hash
Exclusions	On the **Exclusions** tab, you can add objects that you want to exclude from the monitoring scope: • For a File Integrity Monitor rule, you can specify a list of folders. • For a Registry Access Monitoring rule, you can specify registry keys or values. Use masks: **Files** List of files and folders monitored by the component. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders. Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask. The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters. **Registry** Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a mask: Exclusion entries have a higher priority than monitoring scope entries.
Event severity level	Kaspersky Industrial CyberSecurity for Nodes logs file modification events whenever a file or registry key in the monitoring scope is modified. The following event severity levels are available: **Informational**, **Warning**, **Critical**.

On-Demand System Integrity Check

On-Demand System Integrity Check is a task that you can run manually or on a schedule. When running the *Baseline System Integrity Monitor* task, the application compares the current state of the objects included in the monitoring scope with their *baseline* state. A baseline is created when the task is first started.

For System Integrity Monitoring to work, you must add at least one rule. A System Integrity Monitoring rule is a set of criteria that define the access of users to files and the registry. System Integrity Monitoring detects changes in the files and the registry within the specified monitoring scope. The monitoring scope is one of the criteria of a System Integrity Monitoring rule.

Configuring the monitoring scope for the Baseline System Integrity Monitor task

By default, the monitoring scope of the *Baseline System Integrity Monitor* task is the same as the monitoring scope of System Integrity Monitoring. You can configure a different monitoring scope for the task.

System Integrity Monitoring does not support the import of `HKEY_CURRENT_USER` and `HKEY_CURRENT_CONFIG` keys for the *System Integrity Check* task. If the monitoring scope of the task contains these keys, the application generates the *Monitoring scope includes incorrect objects* event.

How to configure a different monitoring scope for the Baseline System Integrity Monitor task in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Tasks**.
2. Select the necessary *Baseline System Integrity Monitor* task and double-click it to open the task properties.
3. In the window that opens, select **Settings**.
4. Configure file monitoring:
   a. Select the **Monitor files** check box on the **Files** tab.
   b. Select rules in the list by selecting check boxes.
   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.
   d. You can also import rules from another source.
5. Configure registry monitoring:
   a. Select the **Monitor the registry** check box on the **Registry** tab.
   b. Select rules in the list by selecting check boxes.
   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.
   d. You can also import rules from another source.
6. Configure external device monitoring:
   a. Select the **Monitor devices** check box on the **Devices** tab.
   b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

      The Baseline System Integrity Monitor task records information about connected external devices at the time when the baseline is created. Subsequently, when an external device is connected, the application generates a corresponding event. When running the task, the application does not monitor the disconnection of external devices.
7. Save your changes.

How to configure a different monitoring scope for the Baseline System Integrity Monitor task in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Select the necessary *Baseline System Integrity Monitor* task and double-click it to open the task properties.
3. In the window that opens, select **Application settings**.
4. Configure file monitoring:
   a. Select the **Monitor files** check box.
   b. Select rules in the list by selecting check boxes.
   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.
   d. You can also import rules from another source.
5. Configure registry monitoring:
   a. Select the **Monitor the registry** check box.
   b. Select rules in the list by selecting check boxes.
   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.
   d. You can also import rules from another source.
6. Configure external device monitoring:
   a. Select the **Monitor devices** check box.
   b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

      The *Baseline System Integrity Monitor* task records information about connected external devices at the time when the baseline is created. Subsequently, when an external device is connected, the application generates a corresponding event. When running the task, the application does not monitor the disconnection of external devices.
7. Save your changes.

How to configure a different monitoring scope for the Baseline System Integrity Monitor task in the Application Console

Properties of the **Baseline System Integrity Monitor** task are editable in the Kaspersky Industrial CyberSecurity for Nodes Console if the task was created locally or if the **Allow use of local tasks** check box is selected in the **Application settings** → **Run local system tasks** section of policy properties.

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection** → **Baseline System Integrity Monitor**.

2. In the results pane of the **Baseline System Integrity Monitor** node, click **Properties**.

   The **Properties: Baseline System Integrity Monitor** window opens.

3. Configure file monitoring:

   a. Select the **Monitor files** check box on the **Files** tab.

   b. Select rules in the list by selecting check boxes.

   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.

   d. You can also import rules from another source.

4. Configure registry monitoring:

   a. Select the **Monitor the registry** check box on the **Registry** tab.

   b. Select rules in the list by selecting check boxes.

   c. If necessary, add a new rule by clicking the **Add** button. Baseline System Integrity Monitor rule settings are described in the following table.

   d. You can also import rules from another source.

5. Configure external device monitoring:

   a. Select the **Monitor devices** check box on the **Devices** tab.

   b. In the **Event severity level** drop-down list, select the importance level of external device monitoring events: *Informational*, *Warning*, *Critical*.

      The Baseline System Integrity Monitor task records information about connected external devices at the time when the baseline is created. Subsequently, when an external device is connected, the application generates a corresponding event. When running the task, the application does not monitor the disconnection of external devices.

6. Save your changes.

Settings of a Baseline System Integrity Monitor task rule

Parameter	Description
Monitor file operations for the scope	The scope to which you want to apply File Integrity Monitoring. This field is mandatory. Use masks: Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders. Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask. The `?` (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.
Monitored objects	Here you can specify the name or value of a registry key. Use masks: Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a mask:
Exclusions	On the **Exclusions** tab, you can add objects that you want to exclude from the monitoring scope: • For a File Integrity Monitor rule, you can specify a list of folders. • For a Registry Access Monitoring rule, you can specify registry keys or values. Use masks: **Files** List of files and folders monitored by the component. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\*\*.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders. Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or folder name, including the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\**\*.txt` will include all paths to files with the TXT extension located in folders nested within the `Folder`, except the `Folder` itself. The mask must include at least one nesting level. The mask `C:\**\*.txt` is not a valid mask. The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters. **Registry** Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a mask: Exclusion entries have a higher priority than monitoring scope entries.
Event severity level	Kaspersky Industrial CyberSecurity for Nodes logs file modification events whenever a file or registry key in the monitoring scope is modified. The following event severity levels are available: **Informational**, **Warning**, **Critical**.

Running the Baseline System Integrity Monitor task

The **Baseline System Integrity Monitor** task allows checking files or registry keys for changes and also checking the connection of external devices. To check files for changes, you can run the **Baseline System Integrity Monitor** task in the following modes:

- **Full Scan**. In this mode, the application checks all attributes and hashes of files.
- **Quick Scan**. In this mode, the application checks only attributes of files.

The mode the task runs in does not affect the checking of the registry or external devices.

How to run the Baseline System Integrity Monitor task in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Tasks**.

   The list of tasks opens.

2. Click **New task**.

   The Task Wizard starts. Follow the instructions of the Wizard.

3. Select **Kaspersky Industrial CyberSecurity for Nodes → Baseline System Integrity Monitor**. Select a System Integrity Monitoring mode:

   - **Full Scan**. In this mode, the application checks all attributes and hashes of files.
   - **Quick Scan**. In this mode, the application checks only attributes of files.

4. Select the computers on which the task will be performed. The following options are available:

   - Select computers detected by the Administration Server in the network: unassigned devices. The specific devices can include devices in administration groups as well as unassigned devices.
   - Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.
   - Specify the selection of devices for which you want to run the task.
   - Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.

5. Select an account to run the task. By default, Kaspersky Industrial CyberSecurity for Nodes starts the task with the rights of a local user account.

6. Configure a schedule for the task, for example, manually or on a certain day of the week.

7. Enter a name for the task.

8. Finish the wizard. If necessary, select the **Run the task after the wizard finishes** check box. You can monitor the progress of the task in the task properties.

How to run a Baseline System Integrity Monitor task in the Web Console

1. In the main window of the Web Console, select **Asset management → Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select Kaspersky Industrial CyberSecurity for Nodes.

   b. In the **Task type** drop-down list, select **Baseline System Integrity Monitor**.

   c. In the **Task name** field, enter a brief description, for example, *Weekly System Integrity Check*.

4. In the **Devices to which the task will be assigned** block, select the task scope.
5. Select devices according to the selected task scope option. Go to the next step.
6. Select the checksum calculation algorithm.
7. Select an account to run the task. By default, Kaspersky Industrial CyberSecurity for Nodes starts the task with the rights of a local user account.
8. Finish the wizard.

   A new task will be displayed in the list of tasks.
9. Click the new task.

   The task properties window opens.
10. Select the **Application settings** tab.
11. Select a System Integrity Check mode:

    - **Full Scan**. In this mode, the application checks all attributes and hashes of files.
    - **Quick Scan**. In this mode, the application checks only attributes of files.
12. Save your changes.
13. Select the check box next to the task.
14. Click **Start**.

Exporting and importing System Integrity Monitoring rules

You can export the list of System Integrity Monitoring rules to an XML file. Then you can modify the file to, for example, add a large number of records of the same type. You can use the export/import function to back up the list of System Integrity Monitoring rules or to migrate the list to a different server.

> System Integrity Monitoring does not support the import of `HKEY_CURRENT_USER` and `HKEY_CURRENT_CONFIG` keys for the *System Integrity Check* task. If the monitoring scope of the task contains these keys, the application generates the *Monitoring scope includes incorrect objects* event.

How to export and import a list of System Integrity Monitoring rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **System Inspection**.
4. In the **System Integrity Monitoring** section, click **Settings**.

5. Depending on which rules you want to export or import, go to the **Files** or **Registry** tab.

6. To export a list of file rules and registry rules:

   a. If you want to export the entire list, click the button and select **Export**.

   b. If you want to export only part of the list, follow these steps:

      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

      2. Click the button and select **Export selected**.

   c. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

7. To import file/registry rules:

   a. Click **Import**.

      In the window that opens, select the XML file from which you want to import the list of rules.

   b. Open the file.

      If the computer already has a list of rules, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

8. Save your changes.

How to export and import a list of System Integrity Monitoring rules in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **System Inspection** → **System Integrity Monitoring** and click the **Configure** button.

   The **System Integrity Monitoring settings** window opens.

5. To export file/registry rules:

   a. On the **File** or **Registry** tab, select the rules that you want to export.

   b. Click the **Export** button.This opens a window; in that window, specify whether you want to export selected rules or all rules, then click **Export**.

      If you did not select any rule, Kaspersky Industrial CyberSecurity for Nodes will export all rules.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

6. To import file/registry rules:

   a. On the **File** or **Registry** tab, click the **Import from the previous version** button if you want to import rules from an XML file created in version 4.0 or earlier of the application.

      If you are importing rules from an XML file created in version 4.5 or later, click **Import**.

b. If the computer already has a list of rules, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

c. In the window that opens, select the XML file from which you want to import the list of rules.

d. Click **Import**.

7. Save your changes.

How to export and import a list of System Integrity Monitoring rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection → System Integrity Monitoring**.

2. In the results pane of the **System Integrity Monitoring** node, click **Properties**.

   The **Properties: System Integrity Monitoring** window opens.

3. Depending on which rules you want to export or import, go to the **Files** or **Registry** tab.

4. To export a list of file rules and registry rules:

   a. If you want to export the entire list, click the button and select **Export**.

   b. If you want to export only part of the list, follow these steps:

      1. Select the list items you want to export using the **CTRL** or **SHIFT** keys. To select all items, press **CTRL+A**.

      2. Click the button and select **Export selected**.

   c. In the window that opens, specify the name of the XML file you want to export to, and select a folder to save the file in. Click the **Save** button.

      Kaspersky Industrial CyberSecurity for Nodes exports the list of rules to the XML file.

5. To import file/registry rules:

   a. Click **Import**.

      In the window that opens, select the XML file from which you want to import the list of rules.

   b. Open the file.

      If the computer already has a list of rules, Kaspersky Industrial CyberSecurity for Nodes will prompt you to delete the existing list or add new entries to it from the XML file.

6. Save your changes.

Viewing System Integrity Monitoring reports

To analyze the performance of System Integrity Monitoring rules, you can look at reports and events generated by the application. Kaspersky Industrial CyberSecurity for Nodes generates the following reports regarding the component:

- Report on computers on which monitoring rules were triggered the greatest number of times
- Report on most frequently triggered monitoring rules

  To generate a Report on most frequently triggered monitoring rules, the application logs the following events:

  - *File or folder change was detected*
  - *Statistics only: prohibited file operation in controlled area*
  - *Allowed file operation in a controlled area performed by a trusted user*
  - *Uncontrolled file operation in controlled area*.

  To configure the storage duration of these events, in the **Event configuration** section of the policy, specify the duration for the general System Integrity Monitoring event: *File or folder change was detected*.

By default, a report is created for the previous 30 days, including the date when the report is created.

How to view System Integrity Monitoring reports in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Reports** tab.
3. Click **New report template**.

   The New Report Template Wizard starts.
4. Follow the instructions of the Report Template Wizard. At the **Selecting the report template type** step, select the a System Integrity Monitoring report (the **Other** section):

   - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   After you have finished with the New Report Template Wizard, the new report template appears in the table on the **Reports** tab.
5. Open the report by double-clicking it.

The report generation process starts. The report is displayed in a new window.

How to view System Integrity Monitoring reports in the Web Console

1. In the main window of the Web Console, select **Monitoring → Reports**.
2. Click **Add**.

   The New Report Template Wizard starts.
3. Under **Template**, in the **Other** section, select a System Integrity Monitoring report:

   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   After you have finished with the New Report Template Wizard, the new report template appears in the table.
4. Select and run the report.

The report generation process starts. The report is displayed in a new window.

To view events generated by the application, you can also use event selections in the Kaspersky Security Center console.

Log Inspection

Log Inspection monitors the integrity of the protected environment based on the Windows event log analysis. When the application detects signs of atypical behavior in the system, it informs the administrator, as this behavior may indicate an attempted cyber attack.

Kaspersky Industrial CyberSecurity for Nodes analyzes Windows event logs and detects violation in accordance with rules. The component includes predefined rules. Predefined rules are powered by heuristic analysis. You can also add your own rules (custom rules). When a rule triggers, the application creates an event with the *Critical* status.

If you want to use Log Inspection, make sure the security audit policy is configured and the system is logging the relevant events (for details, see the Microsoft technical support website.).

Parameter	Description
Predefined rules	List of Log Inspection rules. Predefined rules include templates of abnormal activity on the protected computer. Abnormal activity can signify an attempted attack.
Custom rules	List of Log Inspection rules added by the user. You can set your own Log Inspection rule triggering criteria. To do so, you must enter an event ID and select an event source. You can select an event source from among the standard logs: *Application*, *Security* or *System*. You can also specify the log of a third-party application.

Adding custom rules

You can set your own Log Inspection rule triggering criteria. To do so, you must enter an event ID and select an event source. You can look up the event ID on the Microsoft technical support website. You can select an event source from among the standard logs: *Application*, *Security* or *System*. You can also specify the log of a third-party application. You can find out the name of the third-party application log using the Event Viewer tool. Third-party application logs are kept in the Application and Services Logs folder (for example, the *Windows PowerShell* log).

The application does not check if the specified log is actually present in the Windows event log. If there is a mistake in the name of the log, the application does not monitor events from that log.

The list of custom rules already includes several rules created by Kaspersky experts.

How to add a custom rule in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **System Inspection**.
4. In the **Log Inspection** section, click **Settings**.
5. Select the **Log Inspection** check box.

6. On the **Custom rules** tab, select the **Apply custom rules for Log Inspection** check box.
7. Select the check boxes next to the custom rules that you want to enable.
8. If necessary, click **Add** to create your own custom rules.
9. This opens a window; in that window, configure the custom rule:
   - **Rule name**.
   - **Log name**. Windows Event Logs. The following logs are available: *Application*, *Security*, *System*.
   - **Source**. Third-party application logs. You can find out the name of the third-party application log using the Event Viewer tool. Third-party application logs are kept in the Application and Services Logs folder (for example, the Windows PowerShell log).
   - **Event identifiers**. Event IDs in the Windows Event Log. You can look up the event ID in the Microsoft technical documentation.
10. Save your changes.

How to add a custom rule in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **System Inspection** → **Log Inspection** and click the **Configure** button.
5. Select the **Enable Log Inspection** check box.
6. On the **Custom rules** tab, select the **Apply custom rules for Log Inspection** check box.
7. Configure custom rules using the toggles:
8. If necessary, click **Add** to create your own custom rules.
9. This opens a window; in that window, configure the custom rule:
   - **Rule name**.
   - **Windows Event Log name**. Windows Event Logs. The following logs are available: *Application*, *Security*, *System*.
   - **Source**. Third-party application logs. You can find out the name of the third-party application log using the Event Viewer tool. Third-party application logs are kept in the Application and Services Logs folder (for example, the Windows PowerShell log).
   - **Event ID**. Event IDs in the Windows Event Log. You can look up the event ID in the Microsoft technical documentation.
10. Save your changes.

How to add a custom rule in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection** → **Log Inspection**.
2. In the results pane of the **Log Inspection** node, click **Properties**.

   This opens the **Properties: Log Inspection** window.
3. Select the **Log Inspection** check box.
4. On the **Custom rules** tab, select the **Apply custom rules for Log Inspection** check box.
5. Select the check boxes next to the custom rules that you want to enable.
6. If necessary, click **Add** to create your own custom rules.
7. This opens a window; in that window, configure the custom rule:
   - **Rule name**.
   - **Log name**. Windows Event Logs. The following logs are available: *Application*, *Security*, *System*.
   - **Source**. Third-party application logs. You can find out the name of the third-party application log using the Event Viewer tool. Third-party application logs are kept in the Application and Services Logs folder (for example, the Windows PowerShell log).
   - **Event identifiers**. Event IDs in the Windows Event Log. You can look up the event ID in the Microsoft technical documentation.
8. Save your changes.

As a result, when the rule triggers, Kaspersky Industrial CyberSecurity for Nodes creates *Critical* event.

Configuring predefined rules

Predefined rules include templates of abnormal activity on the protected computer. Abnormal activity can signify an attempted attack. Predefined rules are powered by heuristic analysis. Seven predefined rules are available for Log Inspection. You can enable or disable any of the rules. Predefined rules cannot be deleted.

You can configure the triggering criteria for rules that monitor events for the following operations:

- Password brute-force detection
- Network login detection

How to configure predefined rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **System Inspection**.

4. In the **Log Inspection** section, click **Settings**.

5. Select the **Log Inspection** check box.

6. On the **Predefined rules** tab, select the **Apply predefined rules for Log Inspection** check box.

7. Select or clear check boxes to configure predefined rules:

   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.
   - **Suspicious changes detected in the privileged built-in Administrators group**.

8. If necessary, configure the **There are patterns of a possible brute-force attack in the system** rule:

   a. Click the **Settings** button next to the rule.

   b. In the window that opens, specify the number of attempts and a time period within which attempts to enter a password must be performed for the rule to trigger.

   c. Click **OK**.

9. If you selected the **There is an atypical activity detected during a network logon session** rule, you need to configure its settings:

   a. Click the **Settings** button next to the rule.

   b. In the window that opens, in the **Network logon detection** block, specify the start and the end of the time interval.

      Kaspersky Industrial CyberSecurity for Nodes considers logon attempts performed during the defined interval as abnormal activity.

      By default, the interval is not set and the application does not monitor logon attempts. For the application to continuously monitor logon attempts, set the interval to 12:00 AM – 11:59 PM. The start and the end of the interval must not coincide. If they are the same, the application does not monitor logon attempts.

   c. Create the list of trusted users and trusted IP addresses (IPv4 and IPv6).

      You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts. Kaspersky Industrial CyberSecurity for Nodes does not monitor logon attempts for these users and computers.

Excluding trusted computers by IP address does not work in the application running on Windows XP.

d. Click **OK**.

10. Save your changes.

How to configure predefined rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **System Inspection** → **Log Inspection** and click the **Configure** button.
5. Select the **Enable Log Inspection** check box.
6. On the **Predefined rules** tab, select the **Apply predefined rules for Log Inspection** check box.
7. Configure predefined rules using the toggles:
   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.
   - **Suspicious changes detected in the privileged built-in Administrators group**.
8. On the **Extended** tab, configure the following settings:
   - Number of attempts and a time period within which attempts to enter a password must be performed for the rule **There are patterns of a possible brute-force attack in the system** to trigger.
   - For the **There is an atypical activity detected during a network logon session** rule to trigger, specify the start and end of the time interval during which the application considers all logon attempts as abnormal activity.

     By default, the interval is not set and the application does not monitor logon attempts. For the application to continuously monitor logon attempts, set the interval to 12:00 AM – 11:59 PM. The start and the end of the interval must not coincide. If they are the same, the application does not monitor logon attempts.
9. Create the list of trusted users and trusted IP addresses (IPv4 and IPv6) on the corresponding tabs.

   You can select users from the list of accounts, or enter a local user name manually.

Excluding trusted computers by IP address does not work in the application running on Windows XP.

10. Save your changes.

How to configure predefined rules in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection → Log Inspection**.
2. In the results pane of the **Log Inspection** node, click **Properties**.

   This opens the **Properties: Log Inspection** window.
3. Select the **Log Inspection** check box.
4. On the **Predefined rules** tab, select the **Apply predefined rules for Log Inspection** check box.
5. Select or clear check boxes to configure predefined rules:

   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.
   - **Suspicious changes detected in the privileged built-in Administrators group**.
6. If necessary, configure the **There are patterns of a possible brute-force attack in the system** rule:

   a. Click the **Settings** button next to the rule.

   b. In the window that opens, specify the number of attempts and a time period within which attempts to enter a password must be performed for the rule to trigger.

   c. Click **OK**.
7. If you selected the **There is an atypical activity detected during a network logon session** rule, you need to configure its settings:

   a. Click the **Settings** button next to the rule.

   b. In the window that opens, in the **Network logon detection** block, specify the start and the end of the time interval.

   Kaspersky Industrial CyberSecurity for Nodes considers logon attempts performed during the defined interval as abnormal activity.

   By default, the interval is not set and the application does not monitor logon attempts. For the application to continuously monitor logon attempts, set the interval to 12:00 AM – 11:59 PM. The start and the end of the interval must not coincide. If they are the same, the application does not monitor logon attempts.

c. Create the list of trusted users and trusted IP addresses (IPv4 and IPv6).

You can select users in Active Directory, in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts. Create the list of users from Active Directory. Kaspersky Industrial CyberSecurity for Nodes does not monitor logon attempts for these users and computers.

> Excluding trusted computers by IP address does not work in the application running on Windows XP.

d. Click **OK**.

8. Save your changes.

As a result, when the rule triggers, Kaspersky Industrial CyberSecurity for Nodes creates *Critical* event.

Performance Analyzer

The *Performance Analyzer* task creates a list of the most active application and files that have the most access attempts. This information can help you define a trusted zone to minimize the impact of the application on the performance of industrial software.

For the *Performance Analyzer* task to work correctly, the computer on which the task is started must be running Windows Vista or later.

You can manage this task only in Kaspersky Security Center Web Console and the Application Console.

Task settings and running the Performance Analyzer task in the Kaspersky Security Center Web Console

1. Start the New Task Wizard.
2. In the **Task type** drop-down list, select **Performance Analyzer**.
3. Enter a task name or leave the default name.
4. Select devices to which you want to assign the task and click the **Next** button.
5. In the **Task scope** window, specify a scope for the task and click **Next**.
6. In the **Selecting an account to run the task** window, specify an account and click the **Next** button.
7. In the **Finish task creation** window, select the **Open task details when creation is complete** check box and click **Finish**.
8. This opens a window; in that window, select the **Application settings** tab.
9. Go to the **Performance Analyzer settings** section.
10. In the **Automatically stop the task in** field, set a time interval in hours (1–168 hours) or days (1–7 days) after which Kaspersky Industrial CyberSecurity for Nodes must stop the analysis.
11. If necessary, under **Rule generation scope limitation** create a list of folders in which you want Kaspersky Industrial CyberSecurity for Nodes to perform the analysis to generate exclusion rules:

    Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: You can also add network folders or files to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

    By default, Kaspersky Industrial CyberSecurity for Nodes runs the task without a limited scope.
12. Select the **Schedule** tab and configure a schedule for the task.
13. Save your changes.
14. Select the check box next to the name of the created task and click the **Start** button.

Managing settings and running the Performance Analyzer task in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection** → **Performance Analyzer**.
2. In the results pane, click the **Properties** link.
3. This opens a window; in that window, on the **Task settings** tab, in the **Stop the task in** field, set a time interval in hours (1–168 hours) or days (1–7 days) after which Kaspersky Industrial CyberSecurity for Nodes must stop the analysis.
4. If necessary, under **Rule generation scope** create a list of folders in which you want Kaspersky Industrial CyberSecurity for Nodes to perform the analysis to generate exclusion rules:

   Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: You can also add network folders or files to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

   By default, Kaspersky Industrial CyberSecurity for Nodes runs the task without a limited scope.
5. Go to the **Run mode** tab.
6. Select **Manually** or configure the task run mode.
7. If necessary, under **User**, specify a user account to run the task as.
8. Click **OK** to save the changes.
9. In the **Management** block, click the **Start** link.

You can export *Performance Analyzer* task results directly to the trusted zone settings of a Kaspersky Industrial CyberSecurity for Nodes policy or to local trusted zone settings of the application, or you can save object information from reports to an XML file that you can subsequently import into settings.

Kaspersky Industrial CyberSecurity for Nodes adds files from the report to the list of scan exclusions, and it adds the applications to the list of trusted applications of the trusted zone.

Exporting the results of the Performance Analyzer task in the Kaspersky Security Center Web Console

1. To export local task results:
   a. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
   b. Click the name of the device for which you want to configure task settings.
   c. In the **<Device name>** window that opens, select the **Tasks** tab.
   d. Click the relevant Performance Analyzer task.
2. To export group task results:
   a. In the main window of the Web Console, select **Asset management** → **Tasks**.
   b. Click the relevant Performance Analyzer task.
3. This opens a window; in that window, select the **Application settings** tab.

   The task properties window opens.

4. Go to the **Performance Analyzer results** section.

5. Select the **Consider file hashes** check box to include hash in the report. By default, the check box is cleared.

6. If necessary, clear the **Consider file paths** check box to exclude file paths from the report. The check box is selected by default.

   At least one of the **Consider file hashes**, **Consider file paths** check boxes must be selected.

7. Select objects to be exported on the **Files** and **Applications** tabs.

   You can export the whole report or expand the report and select individual objects that you want to export.

8. To export task results to trusted zone settings of a policy:

   a. Click **Export to settings**.

   b. This opens a window; in that window, select the check box next to the name of the policy to which you want to export settings, then click the **Export** button.

      If a list of exclusions is already configured in the policy, Kaspersky Industrial CyberSecurity for Nodes adds new entries to this list.

9. To export task results to an XML file:

   a. Click **Export to file**.

   b. Click **Export**. This opens a window; in that window, specify whether you want to export selected objects or all objects, then click **Export**.

Exporting Performance Analyzer task results in the Application Console

Export Performance Analyzer of task results to local trusted zone settings of Kaspersky Industrial CyberSecurity for Nodes is available in the Kaspersky Industrial CyberSecurity for Nodes Console if the **Allow use of local exclusions** and **Allow editing of local trusted applications** are selected on the **Scan exclusions** and **Trusted applications** tabs in the **Supplementary** → **Trusted zone** section of the policy.

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **System Inspection** → **Performance Analyzer**.

2. In the results pane, click the **Results** link.

   The **Performance Analyzer results** window opens.

3. Select the **Consider file hashes** check box to include hash in the report. By default, the check box is cleared.

4. If necessary, clear the **Consider file paths** check box to exclude file paths from the report. The check box is selected by default.

   At least one of the **Consider file hashes**, **Consider file paths** check boxes must be selected.

5. Select objects to be exported on the **Files** and **Applications** tabs.

   You can export the whole report or expand the report and select individual objects that you want to export.

6. To export task results to trusted zone settings of the application:

   a. Click **Export to settings**.

   b. Confirm that you want to export the selected objects to trusted zone settings.

      If a list of exclusions is already configured in the settings, Kaspersky Industrial CyberSecurity for Nodes adds new entries to this list.

7. To export task results to an XML file:

   a. Click **Export to file**.

   b. This opens a window; in that window, specify the name of the XML file to which you want to export the list of objects, and select the folder in which you want to save this file.

On-Demand Scan

This section provides information about On-Demand Scan tasks, and instructions on configuring On-Demand Scan task settings and security settings on the protected device.

About On-Demand Scan tasks

Kaspersky Industrial CyberSecurity for Nodes scans the specified area for viruses and other computer security threats. Kaspersky Industrial CyberSecurity for Nodes scans protected device files, RAM, and autorun objects.

Kaspersky Industrial CyberSecurity for Nodes provides the following On-Demand Scan tasks:

- The *Scan at Operating System Startup* task is performed every time Kaspersky Industrial CyberSecurity for Nodes starts. Application scans boot sectors and master boot records of hard drives, removable drives, system memory, and process memory. Every time Kaspersky Industrial CyberSecurity for Nodes runs the task, it creates a copy of non-infected boot sectors. If it detects a threat in those sectors the next time the task starts, it replaces them with the backup copy.

  The *Scan at Operating System Startup* task is created automatically after installation. The **Inform** mode is applied by default. In this case, after you deploy Kaspersky Industrial CyberSecurity for Nodes on the devices, you can enable the *Scan at Operating System Startup* task if no issues with system services were discovered during scan. If the application detects critical system services as infected or probably infected objects, the **Inform** mode gives you time to figure out the reason and solve the issue. Disinfection or removal of the system files may result in critical issues with operating system startup. If the application applies the **Recommended** mode, the following action is performed: **Perform recommended action**.

  > The *Scan at Operating System Startup* task might not be performed if a protected device wakes up after either sleep or hibernate mode. The task is performed only at protected device restart or start up after complete shut down.

- By default, the *Critical Areas Scan* task is performed weekly on a schedule. Kaspersky Industrial CyberSecurity for Nodes scans objects in critical areas of the operating system: autorun objects, boot sectors and master boot records of hard drives and removable drives, system memory and process memory. Kaspersky Industrial CyberSecurity for Nodes applies security settings that correspond to the **Inform** level. You can modify the settings of the *Critical Areas Scan* task.

- The *Application Integrity Control* task is performed daily. It provides the option of checking Kaspersky Industrial CyberSecurity for Nodes modules for damage or modification. The application installation folder is checked. The task execution statistics indicate the number of modules checked and the number of modules found to be corrupted. The values of the task settings are defined by default and cannot be edited. The task start schedule settings can be edited.

- The *Removable Drives Scan* task scans all files that you run or copy, even if the file is located on a removable drive. To prevent the spread of viruses and other malware, you can configure automatic scans of removable drives when they are connected to the computer.

- The *Full Scan* task is performed weekly. The task ensures a thorough scan of the protected device, including system backup storage, boot sectors and mail databases.

Additionally, you can create custom On-Demand Scan tasks, for example, a task for scanning shared folders on the protected device.

Kaspersky Industrial CyberSecurity for Nodes may run several On-Demand Scan tasks at the same time.

About the task scan scope and security settings

In the Application Console, the scan scope of the selected On-Demand Scan task is displayed as a list of the protected device file resources that Kaspersky Industrial CyberSecurity for Nodes can control.

The items or nodes are displayed in a list-view mode of the protected device file resources as follows:

☑ The node is included in the scan scope.

☐ The node is excluded from the scan scope.

Security settings

In the selected On-Demand Scan task, the default security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes or items in the device's file resource list.

> If the same object is included in multiple protection scope entries and these entries have different security levels, the last rule in the list takes priority. For example, consider a protection scope that includes two entries: **All hard drives** (security level **Inform**) and `*\Users\*\Downloads\*` (security level **Custom**). The application scans hard drives in accordance with the Inform level, except the `Downloads` folder. The application scans the `Downloads` folder in accordance with manually specified settings because this entry is the last in the list of the protection scope.

Security settings configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected scan scope or protection scope can be configured using one of the following methods:

- Select one of three predefined security levels (**Maximum performance**, **Recommended**, or **Maximum protection**).
- Manually change the security settings for the selected nodes or items in the list of the protected device's file resources (the security level changes to **Custom**).

Predefined scan scopes

The list of protected device file resources for the selected On-Demand Scan task is displayed in the **Scan scope** window.

> The file resource list displays the nodes to which you have read-access based on the configured Microsoft Windows security settings.

Kaspersky Industrial CyberSecurity for Nodes contains the following predefined scan scopes:

- **All hard drives**. Kaspersky Industrial CyberSecurity for Nodes scans objects on a protected device hard drives. All hard drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **All removable drives**. Kaspersky Industrial CyberSecurity for Nodes scans files on external devices, such as CDs or removable drives. All removable drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **All network drives**. Network folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format. The account used to start the task must have permissions to access the added network folders and files. By default, On-Demand Scan tasks run under the system account.

  Connected network drives will also not be displayed in the protected device's file resource tree. To include objects on network drives in the scan scope, specify the path to the folder that corresponds to this network drive in UNC (Universal Naming Convention) format.

- **Kernel Memory**. Kaspersky Industrial CyberSecurity for Nodes scans the executable files and modules of the processes running in the operating system when the scan is initiated.
- **Running processes and Startup Objects**. Kaspersky Industrial CyberSecurity for Nodes scans objects referred to by registry keys and configuration files, for example WIN.INI or SYSTEM.INI, as well as the application's modules that are started automatically at protected device startup.
- **Disk boot sectors**. Kaspersky Industrial CyberSecurity for Nodes scans boot sectors of hard drives and removable media.
- **System Backup**. Kaspersky Industrial CyberSecurity for Nodes scans the contents of the System Volume Information folder.

  In Kaspersky Industrial CyberSecurity for Nodes 5.0, email is excluded from the application scan scope. If you are using an earlier version of the management plug-in, the application excludes email from the scan scope, even if the policy includes it.

Standard scan scopes are displayed in the tree of network file resources by default. They can be added to the list of network file resources when it is created in the scan scope settings.

By default, On-Demand Scan tasks are run under the following scopes:

- *Scan at Operating System Startup* task:
  - **Kernel Memory**.
  - **Disk boot sectors**.
- *Critical Areas Scan* task:
  - **All hard drives** (excluding Windows folders)
  - **All removable drives**.

- **Kernel Memory**.
- **Running processes and Startup Objects**.

- *On-Demand Scan* task:
  - **All hard drives** (excluding Windows folders)
  - **All removable drives**.
  - **Kernel Memory**.
  - **Running processes and Startup Objects**.
- *Full Scan* task:
  - **All hard drives** (excluding Windows folders)
  - **All removable drives**.
  - **Kernel Memory**.
  - **Running processes and Startup Objects**.
  - **System Backup**.
  - **Disk boot sectors**.

Online storage file scanning

About cloud files

Kaspersky Industrial CyberSecurity for Nodes can interact with Microsoft OneDrive cloud files. The application supports the new OneDrive Files On-Demand feature.

> Kaspersky Industrial CyberSecurity for Nodes does not support other online storages.

OneDrive Files On-Demand helps you access all your OneDrive files without having to download all of them and use storage space on your device. You can download files to your hard drive when you need to.

When the OneDrive Files On-Demand feature is on, you see status icons next to each file in the **Status** column in File Explorer. Each file has one of the following statuses:

This status icon indicates that the file is *only available online*. Online-only files are not physically stored on your hard drive. You can't open online-only files when your device is not connected to the Internet.

This status icon indicates that a file is *locally available*. This happens when you open an online-only file and it downloads to your device. You can open a locally available file anytime, even without Internet access. To clear up space you can change the file back to online-only.

This status icon indicates that a file is *stored on your hard drive and is always available*.

Cloud file scanning

Kaspersky Industrial CyberSecurity for Nodes can only scan cloud files that are stored locally on a protected device. Such OneDrive files have the and statuses. The files are skipped during scanning, since they are not physically located on the protected device.

> Kaspersky Industrial CyberSecurity for Nodes does not automatically download files from the cloud during the scanning, even if they are included in the scan scope.

Cloud files are processed by several Kaspersky Industrial CyberSecurity for Nodes tasks in various scenarios depending on the task type:

- Real-time cloud file scanning: you can add folders containing cloud files to the Real-Time File Protection component protection scope. A file is scanned when it is accessed by the user. If a file is accessed by the user, it is downloaded, becomes locally available, and its status changes to . This allows the file to be processed by the Real-Time File Protection component.
- On-demand cloud file scanning: you can add folders containing cloud files to the On-Demand Scan task's scan scope. The task scans files with the and statuses. If any files are found in the scope, they will be skipped during scanning and an informational event will be recorded in the task log, indicating that the scanned file is only a placeholder for a cloud file and does not exist on a local drive.
- Generating and using applications launch control rules: you can create allowing and denying rules for and files using the *Rule Generator for Applications Launch Control* task. The Applications Launch Control component applies the Default Deny principle and created rules to process and block cloud files.

  > The Applications Launch Control component blocks the start of all cloud files, irrespective of their status. The files are not included in the rule generation scope by the application, as they are not physically stored on your hard drive. Since allowing rules cannot be created for such files, they are subject to the Default Deny principle.

When a threat is detected in a OneDrive cloud file, the application applies the action specified in the settings of the task performing the scanning. Thus, the file may be removed, disinfected, moved to quarantine, or backed up.

> Changes to local files are synchronized with the copies stored on OneDrive in accordance with the principles outlined in the relevant Microsoft OneDrive documentation.

About predefined security levels

> The **Use heuristic analysis** security setting is not included in the settings for the preset security levels. Changing this setting will not change the default security level you have selected.

You can apply one of four predefined security levels to a node selected in the device's file resource tree: **Maximum performance**, **Recommended**, **Maximum protection**, or **Inform**. Each of these levels contains its own predefined security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if your network has additional protected device security measures, for example, firewalls and existing security policies, beyond using Kaspersky Industrial CyberSecurity for Nodes on protected devices and workstations.

Recommended

The **Recommended** security level ensures the best combination of protection and performance impact on devices. Kaspersky experts recommend this level as adequate to protect devices on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization's network has elevated device security requirements.

Inform

The **Inform** security level is recommended if there are potentially many infected computers in the corporate network and blocking them could significantly disrupt the operation of the organization.

Predefined security levels and corresponding security setting values

Options	Security level			
	Maximum performance	Recommended	Maximum protection	Inform
Object types	Objects scanned by format	All objects	All objects	All objects
Scan only new and modified files	Enabled	Disabled	Disabled	Disabled
Action to perform on infected and other objects	Disinfect. Delete if disinfection fails	Perform action recommended by Kaspersky experts	Disinfect. Delete if disinfection fails	Inform
Scan of compound files	Scan distribution packages and files in Microsoft Office formats	Scan all archives, distribution packages and files in Microsoft Office formats	Scan all archives, distribution packages and files in Microsoft Office formats	Scan all archives, distribution packages and files in Microsoft Office formats
System-critical objects are files required for the operation of the operating system and Kaspersky Industrial CyberSecurity for Nodes. These files can not be deleted. Processes associated with such objects cannot be terminated.				
Apply the action to the selected object types	By default, all object types are scanned	By default, all object types are scanned	By default, all object types are scanned	By default, all object types are scanned
Entirely remove the compound file that cannot be modified by the application in case of embedded object detection	No	No	No	No
Exclude files	No	No	No	No
Do not detect objects by type	No	No	No	No
Stop scanning if it takes longer than (sec)	60 sec.	No	No	No

Options	Security level			
	Maximum performance	Recommended	Maximum protection	Inform
Do not scan compound objects larger than (MB)	8 MB	No	No	No
Use iSwift Technology	Yes	Yes	Yes	Yes
Use iChecker technology	Yes	Yes	Yes	Yes

Removable drives scan

You can configure scanning of removable drives connected to the protected device via a USB port.

Kaspersky Industrial CyberSecurity for Nodes scans connected removable drives when they are registered as USB external devices in the operating system. The application does not scan a removable drive if the connection is blocked by the Device Control component.

Kaspersky Industrial CyberSecurity for Nodes allows access to removable drives during scanning.

Scan results for each removable drive are available in the task log for the On-Demand Scan task created when the removable drive is connected.

You can change the settings of the Removable Drives Scan component (see the table below).

Removable Drives Scan settings

Parameter	Default value	Description
Scan removable drives on connection via USB	Cleared	You can turn on or turn off scanning of removable drives when they are connected to the protected device via USB.
Scan removable drive if its size does not exceed (MB)	4096 MB	You can reduce the component's scope by setting the maximum volume of data on the scanned drive. Kaspersky Industrial CyberSecurity for Nodes does not scan a removable drive if the volume of stored data exceeds the specified value.
Scan with security level	Maximum protection	You can configure created On-Demand Scan tasks by selecting one of three security levels: • **Maximum protection** • **Recommended** • **Maximum performance** • **Inform**. The algorithm used when infected, probably infected, and other objects are detected, as well as the other scan settings for each security level, correspond to the predefined security levels in the On-Demand Scan tasks.

Default On-Demand Scan tasks settings

By default On-Demand Scan tasks have the settings described in the table below. You can configure local system and custom On-Demand Scan tasks.

Default On-Demand Scan tasks settings

Parameter	Default value	Description
Scan scope	Applied in local system and custom tasks: • **Scan at Operating System Startup**: the entire protected device, excluding shared folders and autorun objects. • **Critical Areas Scan**: the entire protected device, excluding shared folders and certain operating system files. • **On-Demand Scan** (custom tasks): the entire protected device. • **Full Scan**: a thorough scan of the protected device.	You can change the scan scope. The scan scope cannot be configured for the **Removable Drives Scan** and **Application Integrity Control** local system tasks.
Security settings	Common settings for the entire scan scope correspond to the **Recommended** security level.	For nodes selected in the protected device's file resource list, you can: • Select a different predefined security level • Manually change security settings
Use heuristic analysis	Applied with the **Medium** analysis level for *Critical Areas Scan*, *Scan at Operating System Startup*, *On-Demand Scan* and *Full Scan* tasks.	Heuristic Analyzer can be enabled or disabled and the analysis level can be configured.
Settings to start a task with specific permissions	The task is started under a system account.	You can edit settings to start tasks with specific account permissions for all system and custom On-Demand Scan tasks, except the *Application Integrity Control* task.
Perform task in background mode	Not applied.	You can configure the priority level of On-Demand Scan tasks.
Consider task as Critical Areas Scan	Applied for *On-Demand Scan*, *Scan at Operating System Startup*, *Critical Areas Scan* and *Full Scan* tasks.	You can configure the priority level of On-Demand Scan tasks.
Do not run multiple scan tasks at the same time	Not applied.	You can configure the priority level of On-Demand Scan tasks.
Task start schedule	Applied in local system tasks: • *Scan at Operating System Startup* – **After application startup**. • *Critical Areas Scan*, *Application Integrity Control* and *Full Scan* – **Weekly**.	You can configure the settings for scheduled task startup.

Managing On-Demand Scan tasks

This section describes creating and configuring the *On-Demand Scan* task on the protected device.

Creating an On-Demand Scan task

Creating an On-Demand Scan task in the Kaspersky Security Center Administration Console

1. Start the New Task Wizard.
2. In the **Select task type** window, select **On-Demand Scan** and click **Next**.
3. Create a scan scope in the **Scan scope** window:

By default, the scan scope includes critical areas of the protected device. Scan scopes are marked in the table with the icon ☑. Excluded scan scopes are marked with the ☐ icon in the table. You can change the scan scope: add specific preset scan scopes, disks, folders, network objects and files and assign specific security settings for each scope added.

- To exclude some scope from scanning, select the corresponding list item and click **Delete**.
- To include a predefined scan scope, disk, folder, network object, or file in the scan scope:
  a. Click **Add**.
  b. In the **Select scan scope** window, select the predefined scan scope from the list and click **OK**.
- To exclude subfolders or files from the scan scope:
  a. Select an added folder (or disk) in the **Scan scope** window.
  b. Click **Edit**.
  c. Disable **Include subfolders** checkbox
- To change scan scope security settings:
  a. Select the scan scope for which you want to edit settings and click **Configure**.
  b. This opens a window; in that window, select one of the predefined security levels, or click the **Settings** button to configure security settings manually.

Security settings are configured the same way as for the Real-Time File Protection task.

4. Configure the heuristic analyzer and integration with other components:
   - Configure the use of the heuristic analyzer
   - Select the **Perform task in background mode** check box if you want to assign a *Low* priority to the working process that the task will run in.

     By default, the working processes in which Kaspersky Industrial CyberSecurity for Nodes tasks are run have *Medium* (Normal) priority.

   - Select the **Consider task as Critical Areas Scan** check box if you want to use the task as a *Critical Areas Scan* task.
   - Select the **Do not run multiple scan tasks at the same time** check box to optimize the load on the computer.
5. In the **Select devices to which the task will be assigned** window, specify the list of devices and click **Next**.
6. In the **Selecting an account to run the task** window, specify an account and click **Next**.
7. In the **Configure task schedule** window, configure the task schedule and click **Next**.

8. Enter a name for the task.

   The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

9. The **Finish task creation** window opens. Click the **Finish** button to finish creating the task.

   The new *On-Demand Scan* task will be created for the selected protected device or a group of protected devices.

Creating an On-Demand Scan task in the Kaspersky Security Center Web Console

1. Start the New Task Wizard.
2. In the **New task** window, in the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.
3. In the **Task type** drop-down list, select **On-Demand Scan** and click **Next**.
4. Select the scope of the task and click **Next**.
5. In the **Selecting an account to run the task** window, specify an account and click **Next**.
6. Enter a name for the task.

   The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

7. The **Finish task creation** window opens. Click the **Finish** button to finish creating the task.

   The new *On-Demand Scan* task will be created for the selected protected device or a group of protected devices.

Creating an On-Demand Scan task in the Application Console

Custom tasks for a single protected device can be created in the **On-Demand Scan** node.

To create and configure a new On-Demand Scan task:

1. In the Application Console tree, open the context menu of the **On-Demand Scan** node.
2. Select the **Create task** option.

   The **Create task** window opens.

3. Enter a name for the task and click **OK**.

The *On-Demand Scan* task for an individual protected device is created.

Running an On-Demand Scan task in the background

By default the processes in which Kaspersky Industrial CyberSecurity for Nodes tasks are executed are assigned the *Medium (Normal)* priority.

A process that will run an *On-Demand Scan* task can be assigned *Low* priority. Demoting the process priority increases the time required to execute the task, but may have a beneficial effect on the performance of the processes of other running programs.

Multiple background tasks can be running in a single worker process with low priority.

To change the priority of an existing *On-Demand Scan* task, select or clear the **Perform task in background mode** check box in the task settings.

Configured task settings are saved and applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Registering execution of a Critical Areas Scan

By default, the device protection status is displayed in the results pane of the **Kaspersky Industrial CyberSecurity for Nodes** node and is updated weekly after the *Critical Areas Scan* task is performed.

The time when the device protection status is updated is linked to the schedule of the On-Demand Scan task for which the **Consider task as Critical Areas Scan** check box is selected.

Configuring the scan scope in the On-Demand Scan task

If you modify the scan scope in the *Scan at Operating System Startup* and *Critical Areas Scan* tasks, you can restore the default scan scope for these tasks by repairing Kaspersky Industrial CyberSecurity for Nodes using the Setup Wizard.

Configuring the scan scope for the On-Demand Scan task in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. Double-click to open the properties window of the **On-Demand Scan** task.
6. Select the **Scan scope** section.
7. To add scopes to the scan scope, select check boxes next to them.

8. If you want to add a scan scope that is not on the list:

    a. Click **Add**.

    b. In the displayed window, select a scope, an individual disk, a folder, or a network location.

    c. If you want to include subfolders in the scan scope, select the **Include subfolders** check box.

9. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.

10. To edit a scan scope, select the scan scope in the list and click **Edit**.

11. To hide a previously added scan scope from the list of network file resources, select the scan scope and click **Delete**.

    The scan scope is excluded from the On-Demand Scan task scope when it is removed from the network file resource list.

12. Click **OK**.

The scan scope settings window closes. The newly configured settings are saved.

Configuring the scan scope for the On-Demand Scan task in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

2. Click the name of the computer on which you want to configure the task.

3. Select the **Tasks** section.

4. This opens a window; in that window, double-click to open the properties of the **On-Demand Scan** task.

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

6. To add scopes to the scan scope, enable the switches next to them.

7. If you want to add a scan scope that is not on the list:

    a. Click **Add**.

    b. In the displayed window, select a scope, an individual disk, a folder, or a network location.

    c. If you want to include subfolders in the scan scope, select the **Subfolders** check box.

8. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.

9. To edit a scan scope, select the scan scope in the list and click **Edit scope**.

10. To hide a previously added scan scope from the list of network file resources, select the scan scope and click **Delete**.

    The scan scope is excluded from the On-Demand Scan task scope when it is removed from the network file resource list.

11. Click **Save**.

The scan scope settings window closes. The newly configured settings are saved.

Configuring the scan scope of the On-Demand Scan task in the Application Console

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the results pane of the selected node click the **Configure protection scope** link.
4. In the displayed window, to add scopes to the scan scope, select check boxes next to them.
5. If you want to add a scan scope that is not on the list:
    a. Click **Add**.
    b. In the displayed window, select a scope, an individual disk, a folder, or a network location.
    c. If you want to include subfolders in the scan scope, select the **Include subfolders** check box.
6. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.
7. To edit a scan scope, select the scan scope in the list and click **Edit scope**.
8. To hide a previously added scan scope from the list of network file resources, select the scan scope and click **Delete**.

    The scan scope is excluded from the On-Demand Scan task scope when it is removed from the network file resource list.

9. Click **OK**.

The scan scope settings window closes. The newly configured settings are saved.

Configuring the On-Demand Scan task settings

How to configure the On-Demand Scan task in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
2. In the workspace, select the **Devices** tab.

3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. Double-click to open the properties window of the **On-Demand Scan** task.
6. Select the **Options** section.
7. Clear or select the **Use heuristic analysis** check box.
8. If necessary, change the analysis level.
9. Select the **Perform task in background mode** check box if you want to assign a *Low* priority to the working process that the task will run in.

   By default, the working processes in which Kaspersky Industrial CyberSecurity for Nodes tasks are run have *Medium* (Normal) priority.

10. Select the **Consider task as Critical Areas Scan** check box if you want to use the task as a *Critical Areas Scan* task.
11. Select the **Do not run multiple scan tasks at the same time** check box to optimize the load on the computer.
12. Save your changes.

How to configure the On-Demand Scan task in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
2. Click the name of the computer on which you want to configure the task.
3. Select the **Tasks** section.
4. This opens a window; in that window, double-click to open the properties of the **On-Demand Scan** task.
5. Select the **Application settings** section.
6. Go to the **Settings** section.
7. Clear or select the **Use heuristic analysis** check box.
8. If necessary, select the level of analysis in the **Heuristic analysis level** drop-down list.
9. Select the **Run only when the computer is idle** check box if you want to assign a *Low* priority to the working process that the task will run in.

   By default, the working processes in which Kaspersky Industrial CyberSecurity for Nodes tasks are run have *Medium* (Normal) priority.

10. Select the **Consider task as Critical Areas Scan** check box if you want to use the task as a *Critical Areas Scan* task.

11. Select the **Do not run multiple scan tasks at the same time** check box to optimize the load on the computer.
12. Save your changes.

How to configure the On-Demand Scan task in the Application Console

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the results pane of the selected node, click **Properties**.
4. Select the **Task settings** tab.
5. Clear or select the **Use heuristic analysis** check box.
6. If necessary, change the analysis level.
7. Select the **Perform task in background mode** check box if you want to assign a *Low* priority to the working process that the task will run in.

   By default, the working processes in which Kaspersky Industrial CyberSecurity for Nodes tasks are run have *Medium* (Normal) priority.

8. Select the **Consider task as Critical Areas Scan** check box if you want to use the task as a *Critical Areas Scan* task.
9. Select the **Do not run multiple scan tasks at the same time** check box to optimize the load on the computer.
10. Save your changes.

Configuring Removable Drives Scan

Configuring the Removable Drives Scan in the Kaspersky Security Center Administration Console

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
   In the policy properties window, go to the **Supplementary** section.
5. Click **Settings** in the **Removable Drives Scan** subsection.
   The **Removable Drives Scan** window opens.

6. Do the following:

   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Industrial CyberSecurity for Nodes to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drive if its size does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list, specify the security level with the settings that you want for Removable Drive Scan tasks.

7. Click **OK**.

The specified settings are saved and applied.

Configuring the Removable Drives Scan in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Supplementary** section.
5. Click **Configure** under **Removable Drives Scan**.

   The **Removable Drives Scan** window opens.
6. Do the following:

   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Industrial CyberSecurity for Nodes to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drive if its size does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list, specify the security level with the settings that you want for Removable Drive Scan tasks.

7. Click **OK**.

The specified settings are saved and applied.

Configuring the Removable Drives Scan in the Application Console

1. In the Application Console tree, open the context menu on the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Removable Drives Scan**.

   The **Removable Drives Scan** window opens.

2. Do the following:

   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Industrial CyberSecurity for Nodes to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drive if its size does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list, specify the security level with the settings that you want for Removable Drive Scan tasks.

3. Click **OK**.

Selecting predefined security levels for On-Demand Scan tasks

You can apply one of the following three predefined security levels to a node selected in the protected device's file resource list: **Maximum performance**, **Recommended**, and **Maximum protection**.

Select one of the predefined security levels in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. Double-click to open the properties window of the **On-Demand Scan** task.
6. Select the **Scan scope** section.
7. In the list of the protected device's list, select an item included in the scan scope in order to set a predefined security level.
8. Click **Configure**.
9. This opens a window; in that window, on the **Security level** tab, select the security level to be applied.
10. Click **OK**.
11. In the **Properties: On-Demand Scan** window, click the **OK** button.

Configured task settings are saved and applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Select one of the predefined security levels in the Application Console

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the results pane of the selected node, click **Configure protection scope**.

4. In the network file resource list of the protected device, select a node or item for which you want to set the predefined security level.

5. Make sure that the selected node or item is included in the scan scope.

6. Click **Configure**.

7. This opens a window; in that window, select the security level of your choice.

   The window displays the list of security settings corresponding to the selected security level.

8. Click **OK**.

The task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at the next start.

Configuring security settings manually

By default, On-Demand Scan tasks use common security settings for the entire scan scope.

These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire scan scope or as different settings for different items in the protected device's file resource list or nodes in the tree.

Manually managing security settings in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.

2. In the workspace, select the **Devices** tab.

3. Double-click to open the computer properties window.

4. Go to the **Tasks** section.

5. Double-click to open the properties window of the **On-Demand Scan** task.

6. Select the **Scan scope** section.

7. In the list of protected devices, select an item included in the scan scope to manage security settings.

8. Click **Configure**.

9. This opens a window; in that window, on the **Security level** tab, select the security level to be applied.

10. Select the resource whose security settings you want to configure.

11. Click **Configure**.

12. In the window that opens, select the required security level and click **Settings**.

13. On the **General** tab, specify the following settings:

- Objects that should be included in the protection scope:
  - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.
  - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
  - **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
  - **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.
- In the **Optimization** block, select or clear the **Protect only new and modified files** check box.
- In the **Scan of compound files** section, specify the compound objects that you want to include in the scan scope:
  - **Scan archives**
  - **Scan distribution packages**
  - **Scan files in Microsoft Office formats**
  - **Scan email format files**

14. On the **Actions** tab, specify the following settings:

- Select the action to be performed on infected and other detected objects:
  - **Disinfect**
  - **Disinfect. Delete if disinfection fails**
  - **Delete**
  - **Recommended**
  - **Inform**
- Configure actions to be performed on objects depending on the type of object detected:
  a. Clear or select the **Apply the action to the selected object types** check box.
  b. Click **Settings** and select the types of objects to be detected.
- Configure actions on compound files that are not available for modification: clear or select the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** check box.

15. On the **Optimization** tab, specify the following settings:

    - In the **Exclusions** block:

        - Clear or select the **Exclude files** check box.

        - Clear or select the **Do not detect objects by type** check box.

          Click the **Edit** button for each setting to add exclusions.

    - In the **Advanced settings** block:

        - **Stop scanning if it takes longer than (sec)**

        - **Do not scan compound objects larger than (MB)**

        - **Use iSwift technology**

        - **Use iChecker technology**

16. Save the new security settings.

Manually managing security settings in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

2. Click the name of the computer on which you want to configure the task.

3. Select the **Tasks** section.

4. This opens a window; in that window, double-click to open the properties of the **On-Demand Scan** task.

5. Select the **Application settings** section.

6. Go to the **Scan scope** section.

7. In the network file resource list of the protected device, select an item for which you want to manage security settings. Make sure that the selected item is included in the scan scope.

8. Click **Edit**.

9. Select an objects protection mode in the drop-down list:

    - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.

    - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.

    - **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.

    - **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.

10. Select or clear the **Protect only new and modified files** check box and specify if you want to include Subfolders in the scan.

11. Manage compound object protection settings:

    - **Scan archives**
    - **Scan distribution packages**
    - **Scan files in Microsoft Office formats**
    - **Scan email format files**

12. Select the action to be performed on infected and other detected objects:

    - **Disinfect**
    - **Disinfect. Delete if disinfection fails**
    - **Delete**
    - **Recommended**
    - **Inform**

13. Configure actions to be performed on objects depending on the type of object detected:

    a. Clear or select the **Apply the action to the selected object types** check box.

    b. Click **Settings** and select the types of objects to be detected.

14. Configure actions on compound files that are not available for modification: clear or select the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** check box.

15. In the **Exclusions** block:

    - Clear or select the **Exclude files** check box.
    - Clear or select the **Do not detect objects by type** check box.

16. In the **Add key** block:

    - **Stop scanning if it takes longer than (sec)**
    - **Do not scan compound objects larger than (MB)**
    - **Use iSwift technology**
    - **Use iChecker technology**

17. Save the new security settings.

Manually managing security settings in the Application Console

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the results pane of the selected node, click **Configure protection scope**.
4. In the network file resource list of the protected device, select an item for which you want to manage security settings.
5. Make sure that the selected item is included in the scan scope.
6. Click **Configure**.
7. In the window that opens, select the required security level and click **Settings**.
8. On the **General** tab, specify the following settings:
   - Objects that should be included in the protection scope:
     - **All objects**. Kaspersky Industrial CyberSecurity for Nodes scans all objects.
     - **Objects scanned by format**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file format. Kaspersky compiles the list of formats. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by the list of extensions specified in anti-virus databases**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. Kaspersky compiles the list of extensions. It is included in the Kaspersky Industrial CyberSecurity for Nodes databases.
     - **Objects scanned by specified list of extensions**. Kaspersky Industrial CyberSecurity for Nodes scans only infectable objects based on file extension. The list of extensions is specified manually by the user.
   - In the **Optimization** block, select or clear the **Protect only new and modified files** check box.
   - In the **Scan of compound files** section, specify the compound objects that you want to include in the scan scope:
     - **Scan archives**
     - **Scan distribution packages**
     - **Scan files in Microsoft Office formats**
     - **Scan email format files**
9. On the **Actions** tab, specify the following settings:
   - Select the action to be performed on infected and other detected objects:
     - **Disinfect**
     - **Disinfect. Delete if disinfection fails**
     - **Delete**

- **Recommended**
- **Inform**

- Configure actions to be performed on objects depending on the type of object detected:

  a. Clear or select the **Apply the action to the selected object types** check box.

  b. Click **Settings** and select the types of objects to be detected.

- Configure actions on compound files that are not available for modification: clear or select the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** check box.

10. On the **Optimization** tab, specify the following settings:

- In the **Exclusions** block:

  - Clear or select the **Exclude files** check box.
  - Clear or select the **Do not detect objects by type** check box.

  Click the **Edit** button for each setting to add exclusions.

- In the **Advanced settings** block:

  - **Stop scanning if it takes longer than (sec)**
  - **Do not scan compound objects larger than (MB)**
  - **Use iSwift technology**
  - **Use iChecker technology**

11. Save the new security settings.

On-Demand Scan task statistics

While the *On-Demand Scan* task is being executed, you can view information about the number of objects processed by Kaspersky Industrial CyberSecurity for Nodes since it was started.

This information remains available even if the task is paused. You can view the task statistics in the task log.

To view the On-Demand Scan task statistics:

1. In the Application Console tree, expand the **On-Demand Scan** node.
2. Select the On-Demand Scan task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the results pane of the selected node.

Information about objects processed by Kaspersky Industrial CyberSecurity for Nodes since it was started is presented in the table below.

On-Demand Scan task statistics

Field	Description
Detected	Number of objects detected by Kaspersky Industrial CyberSecurity for Nodes. For example, if Kaspersky Industrial CyberSecurity for Nodes detects one malicious object in five files, the value in this field increases by one.
Infected and other objects	Number of objects that Kaspersky Industrial CyberSecurity for Nodes found and classified as infected or number of found legitimate software files that were not excluded from the scan scope and were classified as legitimate software that can be used by intruders to damage your device or personal data.
Objects not disinfected	Number of objects that Kaspersky Industrial CyberSecurity for Nodes did not disinfect for the following reasons: • The detected object is of a type that cannot be disinfected. • An error occurred during disinfection.
Objects disinfected	Number of objects disinfected by Kaspersky Industrial CyberSecurity for Nodes.
Objects removed	Number of objects successfully deleted by Kaspersky Industrial CyberSecurity for Nodes.
Objects not scanned	Number of objects in the protection scope that Kaspersky Industrial CyberSecurity for Nodes failed to scan, because, for example, access to the object was blocked by another application.
Archives	Number of archives scanned by Kaspersky Industrial CyberSecurity for Nodes.
Packed objects	Number of packed objects scanned by Kaspersky Industrial CyberSecurity for Nodes.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Industrial CyberSecurity for Nodes skipped because they were password protected.
Corrupted objects	Number of objects skipped by Kaspersky Industrial CyberSecurity for Nodes because their format was corrupted.
Processing errors	Number of objects whose processing resulted in an error.
Objects not removed	Number of objects that Kaspersky Industrial CyberSecurity for Nodes attempted to delete unsuccessfully, because, for example, access to the object was blocked by another application.
Objects not processed	Total number of objects that were not processed by Kaspersky Industrial CyberSecurity for Nodes.

You can also view the On-Demand Scan task statistics in the selected task log by clicking the **Open task log** link in the **Management** section of the results pane.

We recommend that you manually process the events recorded on the **Events** tab in the task log upon task completion.

Industrial Network Protection

This section describes the Programmable Logic Controller Project (also referred to as "PLC project") Investigation and Integrity Check tasks and provides instructions on how to configure it.

About PLC Project Integrity Check

This function is designed to check the integrity of PLC projects used in an industrial system.

A PLC project is a microprogram written for a PLC. A PLC project is stored in the PLC's memory and run as part of the production process using the PLC.

PLC Project Integrity Check requires that the protected device network with Kaspersky Industrial CyberSecurity for Nodes installed has access to the PLC.

Before beginning to use this function, perform the following preparatory actions:

1. Obtain information about the PLC projects using the Application Console **PLC Project Investigation** local task.
2. In the Application Console **PLC Project Integrity Check** local task settings, indicate the PLC reference projects from the list of projects obtained in the previous step.

To view information about PLC projects in the PLC Project Integrity Check task,

Open the **Interaction with Administration Server** window in policy properties and select the **Versions of PLC projects** check box to configure data transmission to the Administration Server.

After the *PLC Project Integrity Check* local task is started, the application will issue warnings if the PLC projects have been changed relative to the PLC reference projects.

PLC Project Integrity Check is disabled by default.

Reports

Reporting is one of the basic functions of the Kaspersky Security Center Administration Server. This function can be used only through the Administration Console of Kaspersky Security Center.

After the *PLC Project Integrity Check* task is successfully completed, you can generate and review a report that includes the following information:

- The name of the computer on which the *PLC Project Integrity Check* is completed.
- PLCs, whose integrity is being monitored.

- Last check-up date.
- Results of the integrity check.

To generate a report in the Kaspersky Security Center Administration Server,

Open the Reports tab and select **Report on check of programmable logic controllers (PLCs) for integrity**.

See Kaspersky Security Center Help for detailed information about generating reports.

Configuring PLC Project Integrity Check task

This section provides instructions for configuring general settings of PLC project control tasks.

Configuring PLC Project Investigation

Before running the PLC Project Integrity Check, you must receive information about the PLC projects currently used in the industrial network. Information about PLC projects is obtained using the *PLC Project Investigation* local task.

Configuring PLC Project Investigation in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. In the window that opens, select the **PLC Project Investigation** task and click **Properties**.

   The **Properties: PLC Project Investigation** window opens.
6. Go to **Settings** section, and click the **Add from PLC Registry** button on the **Task settings** tab.

   The **PLC Registry management 5.0.0** window opens.
7. Click **Add**.
8. Under **General settings**, enter the name of the PLC configuration and in the **PLC type** drop-down list, select a PLC type.

   The PLC type represents the model and series provided by a PLC manufacturer.
9. In the **Description** field, enter a PLC description.

   The application links the specified description to each new version of PLC project obtained while running the *PLC Project Investigation* task.
10. In the **Wait for connection** field specify the wait time value (in seconds).

11. Under **Connection settings**, depending on the selected PLC type, fill out the fields: **IP address**, **Port**, **Rack, Telnet port, Controller virtual address**, and **Slot**.

12. If you want to protect connections to the PLC, then, depending on the selected PLC type, select an authentication method:

    - **Password**.

      If the check box is selected, the application will use the password you indicated when connecting to the PLC to query it.

      If the check box is cleared, the application will connect to the PLC without the use of a password. By default, the check box is cleared.

      > The check box will not assign a new password to connect to the PLC. The password must be set up on the side of the PLC.

    - **Use authentication on controller**.

13. Select or clear the **Read data blocks** check box.

    If the check box is selected, the application will take into account the data blocks when calculating the PLC project checksum. It is recommended to select the check box if data blocks contain only statistical values in order to improve the scanning security level.

    If the check box is cleared, the application will not take into account the data blocks. It is recommended not to select the check box if data blocks contain dynamic values to prevent false positives in a *PLC Project Integrity Check* task, while the selected PLC project is compared with a reference project.

    By default, the check box is cleared.

14. Click **OK**.

    > Redundant controllers are not supported.

    The added PLC configurations are displayed on the **Task settings** tab.

15. To add a PLC configuration received after the *PLC Project Investigation* task on the local computer with the Kaspersky Industrial CyberSecurity for Nodes Console installed completes:

    a. In the list of PLC configurations, select one that you want to add to the PLC Registry.

    b. Click **Link to PLC Registry**.

    > Each PLC configuration from the Registry has a unique ID number specified in the last column. After you add a PLC configuration from the local computer task to the PLC Registry, an ID number will be assigned to this configuration.

16. Click **Delete** if you want to delete the selected PLC configuration from the task list.

    > The PLC configuration is not deleted from the PLC Registry and can be added again at any moment.

17. Save your changes.

The PLC project information obtained as a result of running the *PLC Project Investigation* task is used to select PLC reference projects and to configure the *PLC Project Integrity Check* task.

Configuring PLC Project Investigation in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.
2. Click the name of the computer on which you want to configure the *PLC Project Investigation* task.
3. Select the **Tasks** tab.
4. This opens a window; in that window, double-click to open the properties of the **PLC Project Investigation** task.
5. Select the **Application settings** tab and click **Add from PLC Registry**.

   The **PLC configuration** window opens.
6. In the **PLC settings** section, in the **PLC type** drop-down list, select the PLC type.

   The PLC type represents the model and series provided by a PLC manufacturer.
7. In the **Description** field, enter a PLC description.

   The application links the specified description to each new version of PLC project obtained while running the *PLC Project Investigation* task.
8. In the **Connection timeout, sec** field specify the wait time value (in seconds).
9. In the **Connection settings** section, depending on the selected PLC type, fill out the fields: **Controller address**, **Port**, **Rack, Telnet port, Controller virtual address**, and **Slot**.
10. If you want to protect connections to the PLC, then, depending on the selected PLC type, select an authentication method:

    - **Apply password**.

      If the check box is selected, the application will use the password you indicated when connecting to the PLC to query it.

      If the check box is cleared, the application will connect to the PLC without the use of a password. By default, the check box is cleared.

      > The check box will not assign a new password to connect to the PLC. The password must be set up on the side of the PLC.

    - **Use authentication on controller**.
11. Select or clear the **Read data blocks** check box.

    If the check box is selected, the application will take into account the data blocks when calculating the PLC project checksum. It is recommended to select the check box if data blocks contain only statistical values in order to improve the scanning security level.

    If the check box is cleared, the application will not take into account the data blocks. It is recommended not to select the check box if data blocks contain dynamic values to prevent false positives in a *PLC Project Integrity Check* task, while the selected PLC project is compared with a reference project.

    By default, the check box is cleared.

12. Click **OK**.

    Redundant controllers are not supported.

    The added PLC configurations are displayed on the **Application settings** tab.

13. To add a PLC configuration received after the *PLC Project Investigation* task on the local computer with the Kaspersky Industrial CyberSecurity for Nodes Console installed completes:

    a. In the list of PLC configurations, select one that you want to add to the PLC Registry.

    b. Click **Link to PLC Registry**.

    Each PLC configuration from the Registry has a unique ID number specified in the last column. After you add a PLC configuration from the local computer task to the PLC Registry, an ID number will be assigned to this configuration.

14. Click **Delete** if you want to delete the selected PLC configuration from the task list.

    The PLC configuration is not deleted from the PLC Registry and can be added again at any moment.

15. Save your changes.

Configuring PLC Project Investigation in the Application Console

1. In the Application Console tree, expand the **Industrial Network Protection** node.
2. Select the **PLC Project Investigation** child node.
3. Click the **Properties** link in the details pane of the **PLC Project Investigation** node.

   The **Properties: PLC Project Investigation** window opens.
4. On the **Task settings** tab, click the **Add** button.

   The **PLC configuration** window opens.
5. Under **General settings** in the **PLC type** drop-down list, select the PLC type.

   The PLC type represents the model and series provided by a PLC manufacturer.
6. In the **Description** field, enter a PLC description.

   The application links the specified description to each new version of PLC project obtained while running the *PLC Project Investigation* task.
7. In the **Wait for connection** field specify the wait time value (in seconds).
8. Under **Connection settings**, depending on the selected PLC type, fill out the fields: **IP address**, **Port**, **Rack, Telnet port, Controller virtual address**, and **Slot**.

9. If you want to protect connections to the PLC, then, depending on the selected PLC type, select an authentication method:

   - **Password**.

     If the check box is selected, the application will use the password you indicated when connecting to the PLC to query it.

     If the check box is cleared, the application will connect to the PLC without the use of a password. By default, the check box is cleared.

     > The check box will not assign a new password to connect to the PLC. The password must be set up on the side of the PLC.

   - **Use authentication on controller**.

10. Select or clear the **Read data blocks** check box.

    If the check box is selected, the application will take into account the data blocks when calculating the PLC project checksum. It is recommended to select the check box if data blocks contain only statistical values in order to improve the scanning security level.

    If the check box is cleared, the application will not take into account the data blocks. It is recommended not to select the check box if data blocks contain dynamic values to prevent false positives in a *PLC Project Integrity Check* task, while the selected PLC project is compared with a reference project.

    By default, the check box is cleared.

11. Click **OK**.

    > Redundant controllers are not supported.

    The added PLC configurations are displayed on the **Task settings** tab.

12. Click **Delete** if you want to delete the selected PLC configuration from the task list.

    > The PLC configuration is not deleted from the PLC Registry and can be added again at any moment.

13. Save your changes.

The PLC project information obtained as a result of running the *PLC Project Investigation* task is used to select PLC reference projects and to configure the *PLC Project Integrity Check* task.

Configuring PLC Project Integrity Check

Configuring PLC Project Integrity Check in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.

2. In the workspace, select the **Devices** tab.

3. Double-click to open the computer properties window.

4. Go to the **Tasks** section.

5. In the window that opens, select the **PLC Project Integrity Check** task and click **Properties**.

   The **Properties: PLC Project Integrity Check** window opens.

6. Go to the **Settings** section.

7. In the window that opens, click the **Add** button to add to the list the configurations for which the *PLC Project Integrity Check* task will be run.

   The **Data for PLC Project Integrity Check** window opens.

   All information in this window is obtained as a result of running the Kaspersky Security Center's *PLC Project Investigation* task.

8. In the **PLC type** drop-down list, select the PLC type whose project integrity you want to check.

9. From the list, select a configuration for the selected PLC type and specify the reference version for the PLC project. Based on the results of a comparison with the PLC reference project's settings, the application makes a conclusion regarding the integrity of the PLC project.

10. In the **Data for PLC Project Integrity Check** window, click **OK** to save your changes. PLC project information is added to the task.

11. Select the added PLC configuration in the list in the **Properties: PLC Project Integrity Check** window.

    - The **PLC configuration** tab displays information about the hash of the PLC project and the date on which it was received.

    - The **Reference version of PLC project** tab contains detailed information about the PLC configuration**.**

12. Save your changes.

Configuring PLC Project Integrity Check in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

2. Click the name of the computer on which you want to configure the *PLC Project Integrity Check* task.

3. Select the **Tasks** section.

4. This opens a window; in that window, double-click to open the properties of the **PLC Project Integrity Check** task.

5. Select the **Application settings** tab and click **Add**.

   The **Data for PLC Project Integrity Check** window opens.

   All information in this window is obtained as a result of running the Kaspersky Security Center's *PLC Project Investigation* task.

6. Click **Select PLC configuration** to select a PLC configuration.

7. Select a time interval that the application must observe when requesting information about PLC projects.

8. Click **Select reference PLC project** and specify the reference version for the PLC project.
   Based on the results of a comparison with the PLC reference project's settings, the application makes a conclusion regarding the integrity of the PLC project.

9. Click **OK** to save the changes.
10. Select the added PLC configuration in the list.
11. Save your changes.

Configuring PLC Project Integrity Check in the Application Console

1. In the Application Console tree, expand the **Industrial Network Protection** node.
2. Select the **PLC Project Integrity Check** child node.
3. Click the **Properties** link in the details pane of the **PLC Project Integrity Check** node.

   The **Schedule and run mode** window opens.
4. In the window that opens, configure the following settings:

   - Manage the task schedule settings.
   - If necessary, enable the **Run task with user rights** functionality and specify the user name and password of the user whose account you want to use to run the task.
5. Click the **Configure protection scope** link in the results pane of the **PLC Project Integrity Check** node.
6. In the window that opens, click the **Add** button to add to the list the configurations for which the *PLC Project Integrity Check* task will be run.

   The **Data for PLC Project Integrity Check** window opens. All information in this window is obtained as a result of running the Kaspersky Security Center's *PLC Project Investigation* task.
7. In the **PLC type** drop-down list, select the PLC type whose project integrity you want to check.
8. From the list, select a configuration for the selected PLC type and specify the reference version for the PLC project. Based on the results of a comparison with the PLC reference project's settings, the application makes a conclusion regarding the integrity of the PLC project.
9. In the **Data for PLC Project Integrity Check** window, click **OK** to save your changes. PLC project information is added to the task.
10. Select the added PLC configuration in the list in the **Properties: PLC Project Integrity Check** window.

    - The **PLC configuration** tab displays information about the hash of the PLC project and the date on which it was received.
    - The **Reference version of PLC project** tab contains detailed information about the PLC configuration.
11. Save your changes.

Enabling and Disabling PLC Project Integrity Check

The *PLC Project Integrity Check* task is run only after Kaspersky Industrial CyberSecurity for Nodes receives firmware information using the *PLC Project Investigation* task.

Enabling or disabling PLC Project Integrity Check in the Kaspersky Security Center Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
2. In the workspace, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Tasks** section.
5. In the window that opens, select the **PLC Project Investigation** task and perform one of the following actions:
   - To enable PLC Project Integrity Check, in the context menu of the task, select **Start**.
     The *PLC Project Integrity Check* task is started.
   - To disable PLC Project Integrity Check, in the context menu of the task, select **Stop**.
     The *PLC Project Integrity Check* task is stopped.

Enabling or disabling PLC Project Integrity Check in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.
2. Click the name of the computer on which you want to configure the *PLC Project Integrity Check* task.
3. Select the **Tasks** tab.
4. Select the check box next to the **PLC Project Investigation** task and do one of the following:
   - To enable PLC Project Integrity Check, click the **Start** button.
     The *PLC Project Integrity Check* task is started.
   - To disable PLC Project Integrity Check, click the **Stop** button.
     The *PLC Project Integrity Check* task is stopped.

Enabling or disabling PLC Project Integrity Check in the Application Console

1. In the Application Console tree, expand the **Industrial Network Protection** node.
2. Select the **PLC Project Investigation** child node.
3. In the **Management** section of the details pane of the **PLC Project Investigation** node, click the **Start** link.
4. Select the **PLC Project Integrity Check** child node.
5. In the **Management** section of the details pane of the **PLC Project Integrity Check** node, perform one of the following steps:
   - To enable PLC Project Integrity Check, click the **Start** link.
     The *PLC Project Integrity Check* task is started.
   - To disable PLC Project Integrity Check, click the **Stop** link.
     The *PLC Project Integrity Check* task is stopped.

About the PLC configurations Registry

The PLC configurations Registry (also referred to as Registry) is a shared list of all PLC configurations that are used by Kaspersky Industrial CyberSecurity for Nodes. *PLC configuration* is a set of individual properties of a PLC, which can be specified in settings (IP address, rack number, model, etc.). You can add, modify and remove PLC configurations while working with the Registry.

In Kaspersky Industrial CyberSecurity for Nodes 4.5, the procedure for calculating the hash of configuration for PLCs of the Siemens SIMATIC S7-300 / 400 / 400H type has changed. Therefore, after upgrading the application, you must restart the *PLC Project Investigation* task to create new baselines for these PLC projects.

The PLC configurations Registry can be filled manually or by importing a configuration file containing PLC configuration data.

The list of PLC configurations in the Registry is used for creating a protection scope of the *PLC Project Integrity Check* task, configured via the Kaspersky Security Center Administration Console. When creating the *PLC Project Investigation* task list you can add and remove PLC configurations, that were added to the Registry. If you remove a PLC configuration from the task list, this configuration is not removed from the Registry.

Each PLC configuration added to the Registry acquires a unique identification number. If the PLC configuration is altered, the identification number changes. PLC configurations, that are added in a list of the *PLC Project Investigation* task in the Kaspersky Industrial CyberSecurity for Nodes Console, do not have any identification numbers. Such PLC configurations can be added to the Registry manually when creating a *PLC Project Investigation* task protection scope in the Kaspersky Security Center.

The list of PLC configurations of the *PLC Project Investigation* task in Kaspersky Security Center is populated from two sources:

- PLC configurations without IDs, added to the list of a local task via the Application Console (the lists are synchronized automatically);
- PLC configurations with IDs, added from the Registry by the administrator.

If the PLC configuration added to the *PLC Project Investigation* task list is removed from the Registry, Kaspersky Industrial CyberSecurity for Nodes notifies you that the integrity check results might be distorted. Make sure that all PLC configurations in the *PLC Project Investigation* task list exist in the Registry and restart the PLC Project Investigation task.

Configuring PLC Registry

To configure the PLC registry:

1. Open the **PLC Registry management** window in one of the following ways:

   - **From the settings of the local PLC Project Investigation task**

     1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
     2. In the workspace, select the **Devices** tab.
     3. Double-click to open the computer properties window.
     4. Go to the **Tasks** section.
     5. In the window that opens, select the **PLC Project Investigation** task and click **Properties**.

        The **Properties: PLC Project Investigation** window opens.
     6. Go to **Settings** section, and click the **Add from PLC Registry** button on the **Task settings** tab.

        The **PLC Registry management 5.0.0** window opens.

   - **From the Kaspersky Security Center Administration Console Hardware folder**

     a. In the Kaspersky Security Center Administration Console tree, expand the **Administration Server <server name>** node.

     b. Expand the **Advanced** node.

     c. In the **Repositories** folder, select the **Hardware** nested folder.

     > If you cannot see a **Hardware** folder, select the **Display Vulnerability and patch management** check box in the Administration Server interface settings.

     d. In the workspace of the **Hardware** folder, in the context menu of the **Additional actions** button, select **PLC Registry management 5.0.0**.

        The **PLC Registry management 5.0.0** window opens.

2. Manually add the required PLC configurations.

3. If required, **import PLC project configuration data from an XML file**.

   a. Click **Import**.

      The standard Microsoft Windows **Open File** window opens.

   b. Specify the path to the PLC settings XML file.

c. Click **Open**.

The new PLC configuration data entries appear in the list in the **PLC Registry management** window.

4. If required, **export the PLC project configuration data to an XML file**.

a. Click **Export**.

b. In the pop-up window, provide the location and filename for the XML file where you wish to save the PLC project configuration data.

c. Click the **Save** button.

5. To change the PLC configuration settings, click **Edit**.

When you modify the PLC configuration in the PLC Registry, the results of the *PLC Project Integrity Check* task are affected. You need to run the *PLC Project Investigation* task to get the updated data and then run the *PLC Project Integrity Check* again to get actual results.

1. Click the **Delete** button, if you do not use the PLC Project configuration any more.

> When the PLC project is deleted from the PLC Registry, it becomes unavailable for further investigation and integrity check.

2. Use the **Filter** field to review the PLC configurations with the required values.

3. If required, select the **Show only PLC configurations, that can be protected by Kaspersky Industrial CyberSecurity for Nodes** check box.

4. Click **Close**.

The PLC Registry will be saved.

Security audit

The task can be run only if you have an active Kaspersky Industrial CyberSecurity for Node license key with an ICS Audit licensed object.

Security Audit task is a group or local task intended to search for vulnerabilities on devices and assess devices' compliance with operating system standards. To perform a Security Audit task, Kaspersky Industrial CyberSecurity for Nodes uses databases in XML format supplied with the product or custom ones.

- To search for vulnerabilities on devices, the application uses rules written in the OVAL language.
- To assess device security and standards compliance for operating systems, the application uses rule configurations written in the OVAL and XCCDF languages.

Security Audit rules are divided into classes:

- Compliance – these rules check the system configuration settings for compliance with the security policy.
- Inventory – these rules check whether the software or hardware specified in the rules is present in the system.
- Miscellaneous – these rules contain custom checks.
- Patch – these rules check whether the patches specified in the rules are installed on the system.
- Vulnerability – these rules check whether the vulnerabilities specified in the rules are present in the system.

Limitations for Security Audit task settings

When creating and configuring Security Auditing tasks, consider the following limitations:

- Aggregate limit of 2 MB on the cumulative size of files used when selecting a **Custom rule base from file** source.
- The limit on the size of the report on the task execution results is 7.5 MB.

Supported OVAL scan types

The following types of OVAL scans are supported for the Security Audit task:

- accesstoken
- auditeventpolicy
- auditeventpolicysubcategories
- cmdlet – available for Windows Vista / Server 2008 and later

- environmentvariable58
- environmentvariable
- family
- file
- fileauditedpermissions53
- filehash58
- filehash
- group_sid
- interface
- lockoutpolicy
- passwordpolicy
- port
- process58
- process
- registry
- rpmverifyfile
- service
- sid
- textfilecontent54
- user
- user_sid
- variable
- wmi57
- wmi
- xmlfilecontent

For unsupported OVAL scans, errors will be displayed in the security audit results report.

Managing Security Audit tasks

The task can be run only if you have an active Kaspersky Industrial CyberSecurity for Node license key with an ICS Audit licensed object.

Security Audit tasks are local or group tasks that are created and configured using Kaspersky Security Center Web Console or the command line interface. These tasks are used to search for vulnerabilities and assess the compliance of enterprise systems with security standards.

This section provides instructions on how to manage Security Audit tasks.

Creating and configuring the Security Audit task with the default settings

To create and configure the Security Audit task with the default settings:

1. Select **Asset management** → **Tasks** in the main window of Kaspersky Security Center Web Console.
2. Click **Add**.
   The Task Wizard starts.
3. In the **Application** drop-down list, select Kaspersky Industrial CyberSecurity for Nodes.
4. In the **Task type** drop-down list, select **Security Audit**.
5. Enter a task name or leave the default name.
6. Select devices to which the task will be assigned.
7. Click **Next**.
8. In the **Selecting an account to run the task** window, do one of the following:
   - Select the default account.
   - Enter the name and password of the user whose account permissions will be used to start the task.
9. Click **Next**.
10. In the **Finish task creation** window, select the **Open task details when creation is complete** check box.
11. Click **Finish**.
    The task properties window will open, containing the default settings.
12. Open the **Application settings** tab.
    In the **Source of rules** section, the **Custom rule base from file** is selected by default.

13. Click the **Import rule base from file** button.

14. In the window that opens, specify the file with the rule database.

    You can load only one archive containing an XML file with OVAL rules and XCCDF rules.

    > The total archive size must not exceed 2 MB.

15. Click **Open**.

    The **Source of rules** section displays information about the loaded rules. Follow the **Learn more** link in the **Platforms** field to open the window with the list of operating systems and products mentioned in the rules of the selected source.

16. If necessary, load the file with external variables.

    > You cannot use external variables if the selected rule source contains XCCDF rules.

    a. Select the **Use external variables data with custom database** check box.

    b. Click the **Import external variables from file** link.

    c. In the window that opens, specify the path to the file with the external variables.

    d. Click **Open**.

17. In the **Scope** section, if necessary, change the vulnerability scan mode:

    > The **Scope** section is unavailable if the selected rule source contains XCCDF rules.

    a. Select one of the modes:

    - **Scan all vulnerabilities**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the vulnerabilities database.

    - **Scan all vulnerabilities except added to the list**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the vulnerabilities database except for those added to the list below.

    - **Scan vulnerabilities added to the list**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect vulnerabilities added to the list below.

    b. If you selected **Scan all vulnerabilities except added to the list** or **Scan vulnerabilities added to the list**, create a list of vulnerabilities using the **Add** or **Add by conditions** buttons.

18. In the **Advanced settings** section, if necessary, determine the statuses of directive-based scans that will be included in the Security Audit task report:

Directives cannot be applied if the selected rule source contains XCCDF rules.

a. Select the **Use Directives** check box.

b. Using the switch next to each directive, determine the statuses of directive-based scans that will be displayed in the Security Audit task report.

If the switch next to a directive status is on, results of scans based on the directive's rules that have this status will be displayed in the Security Audit task report.

By default, the check boxes next to the **True** and **False** scan results are selected for all directives.

19. In the **Advanced settings** section, if necessary, configure settings for logging task completion events:

a. Select the **Enable logging** check box.

b. Select the desired **Logging level** from the list.

By default, the log is stored in the C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs folder.

The following logging levels are available:

- **Critical level** – only Critical events
- **Warning level** – only Critical and Warning events
- **Information level** – all Critical, Warning and Information events
- **Debug level** – all Critical, Warning, Information and Debug events

20. Click **Save** to save the changes.

You can start the created task manually or configure a scheduled task start. See Kaspersky Security Center Help for more details.

Configuring Security Audit task settings using the Kaspersky ICS CERT vulnerabilities database for SCADA

The Kaspersky ICS CERT vulnerabilities database for SCADA is provided and updated together with updates of Kaspersky Industrial CyberSecurity for Nodes databases and modules. Accordingly, before configuring the Security Audit task settings using the Kaspersky ICS CERT vulnerabilities database for SCADA as a rule source, update the application databases and modules.

To configure Security Audit task settings using the Kaspersky ICS CERT vulnerabilities database for SCADA as a rule source:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the name of the Security Audit task.
3. Select the **Application settings** tab.

4. In the **Source of rules** section, select **Kaspersky ICS CERT vulnerabilities database for SCADA**.

   Information about the vulnerability database is displayed. Follow the **Details** link in the **Platforms** field to open the window with the list of operating systems and products mentioned in the rules of the selected source.

5. In the **Scope** section, if necessary, change the vulnerability scan mode:

   a. Select one of the modes:

   - **Scan all vulnerabilities**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the Kaspersky ICS CERT vulnerabilities database for SCADA.

   - **Scan all vulnerabilities except added to the list**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the Kaspersky ICS CERT vulnerabilities database for SCADA except for those added to the list below.

   - **Scan vulnerabilities added to the list**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect vulnerabilities added to the list below.

   b. If you selected **Scan all vulnerabilities except added to the list** or **Scan vulnerabilities added to the list**, create a list of vulnerabilities using the **Add** or **Add by conditions** buttons.

6. In the **Advanced settings** section, if necessary, determine the statuses of directive-based scans that will be included in the Security Audit task report:

   a. Select the **Use Directives** check box.

   b. Using the switch next to each directive, determine the statuses of directive-based scans that will be displayed in the Security Audit task report.

   If the switch next to a directive status is on, results of scans based on the directive's rules that have this status will be displayed in the Security Audit task report.

   By default, the check boxes next to the **True** and **False** scan results are selected for all directives.

7. In the **Advanced settings** section, if necessary, configure settings for logging task completion events:

   a. Select the **Enable logging** check box.

   b. Select the desired **Logging level** from the list.

   By default, the log is stored in the C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs folder.

   The following logging levels are available:

   - **Critical level** – only Critical events
   - **Warning level** – only Critical and Warning events

- **Information level** – all Critical, Warning and Information events
- **Debug level** – all Critical, Warning, Information and Debug events

8. Click the **Save** button to save the task settings.

Configuring Security Audit task settings using a security and standards compliance configuration

Security and standards compliance configurations are set and updated together with Kaspersky Industrial CyberSecurity for Nodes database and module updates. Accordingly, before you configure Security Audit task settings using a security and standards compliance configuration, update the application databases and modules.

To configure Security Audit task settings using a security and standards compliance configuration as the rule source:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the name of the Security Audit task.
3. Select the **Application settings** tab.
4. In the **Source of rules** section, select **Compliance and security configurations for operating systems**.
5. Click **Select configuration of rules**.
6. In the window that opens, select one of the security and standards compliance configurations.
7. Click **OK**.

   The **Source of rules** selection displays information about the selected security and standards compliance configuration. The **Rules** section displays the list of rules included in the security and standards compliance configuration selected as a source.
8. In the **Advanced settings** section, if necessary, configure settings for logging task completion events:
   a. Select the **Enable logging** check box.
   b. Select the desired **Logging level** from the list.

      By default, the log is stored in the C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs folder.

      The following logging levels are available:

      - **Critical level** – only Critical events
      - **Warning level** – only Critical and Warning events
      - **Information level** – all Critical, Warning and Information events
      - **Debug level** – all Critical, Warning, Information and Debug events

9. In the **Rules** section, review the list of rules included in the selected security and standards compliance configuration:
   - Click the rule name to open the rule description.
   - Click the **Filter** button to open the window for filtering rules.
10. Click the **Save** button to save the task settings.

Configuring Security Audit task settings using a custom rule database from the Kaspersky Security Center repository

Before configuring Security Audit task settings using custom databases using the Kaspersky Security Center repository:

1. Create a thumbprint for the certificate for signing the custom database from the command line interface.

   You can use an existing thumbprint for the certificate for signing the custom database.

2. Create a Kaspersky Security Center installation package named package.zip using the command line interface.
3. Add the package.zip archive with OVAL and XCCDF rules created at the previous step to the Kaspersky Security Center repository. To do so, create and run the task to install the installation package with the following settings:
   - The installation package must be created base on files from the package.zip archive that was created at the previous step.
   - In the window for selecting devices to which you will assign the task for installing the installation package, manually specify the address of the computer on which Kaspersky Security Center Administration Server is installed.

In Kaspersky Industrial CyberSecurity for Nodes, you can only update an installed and deployed package with a custom rule database. The rule package cannot be deleted.

To configure Security Audit task settings using a custom rule database from the Kaspersky Security Center repository:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the task name.
3. Select the **Application settings** tab.
4. In the **Source of rules** section, select **Custom rule base from Kaspersky Security Center repository**.
5. Click the **Select file from custom collection** button.
6. In the window that opens, specify the archive with the rule database.

   You can load only one archive containing an XML file with OVAL rules and/or XCCDF rules.

The total archive size must not exceed 2 MB.

7. Click **Open**.

   The **Source of rules** section displays information about the loaded rules. Follow the **Details** link in the **Platforms** field to open the window with the list of operating systems and products mentioned in the rules of the selected source.

8. If necessary, specify the thumbprint of the certificate for signing the custom rule database:

   a. Select the **Use thumbprint** check box. If this functionality is enabled, Kaspersky Security Center will check the thumbprint when executing the task. If the thumbprint does not match the one specified in the task settings, the task execution will terminate with an error.

   If this functionality is disabled, Kaspersky Security Center will not check the thumbprint.

   b. In the **Thumbprint** field, enter the thumbprint obtained using the command line interface.

9. If necessary, load the file with external variables

   You cannot use external variables if the selected rule source contains XCCDF rules.

   a. Select the **Use external variables data with custom database** check box.

   b. Click **Import external variables from file**.

   c. In the window that opens, specify the path to the file with the external variables.

   d. Click **OK**.

10. In the **Scope** section, if necessary, change the vulnerability scan mode:

    The **Scope** section is unavailable if the selected rule source contains XCCDF rules.

    a. Select one of the modes:

    - **Scan all vulnerabilities**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the Kaspersky ICS CERT vulnerabilities database for SCADA.

    - **Scan all vulnerabilities except added to the list**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the Kaspersky ICS CERT vulnerabilities database for SCADA except for those added to the list below.

    - **Scan vulnerabilities added to the list**.

      Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect vulnerabilities added to the list below.

    b. If you selected **Scan all vulnerabilities except added to the list** or **Scan vulnerabilities added to the list**, create a list of vulnerabilities using the **Add** or **Add by conditions** buttons.

11. In the **Advanced settings** section, if necessary, determine the statuses of directive-based scans that will be included in the Security Audit task report:

    Directives cannot be applied if the selected rule source contains XCCDF rules.

    a. Select the **Use Directives** check box.

    b. Using the switch next to each directive, determine the statuses of directive-based scans that will be displayed in the Security Audit task report.

    If the switch next to a directive status is on, results of scans based on the directive's rules that have this status will be displayed in the Security Audit task report.

    By default, the check boxes next to the **True** and **False** scan results are selected for all directives.

12. In the **Advanced settings** section, if necessary, configure settings for logging task completion events:

    a. Select the **Enable logging** check box.

    b. Select the desired **Logging level** from the list.

    By default, the log is stored in the C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs folder.

    The following logging levels are available:

    - **Critical level** – only Critical events
    - **Warning level** – only Critical and Warning events
    - **Information level** – all Critical, Warning and Information events
    - **Debug level** – all Critical, Warning, Information and Debug events

13. Click the **Save** button to save the task settings.

Configuring the Security Audit task settings using a custom database from file

To configure the Security Audit task settings using a custom database from a file:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the task name.
3. Open the **Application settings** tab.
4. In the **Source of rules** section, select **Custom rule base from file**.
5. Click the **Import rule base from file** button.
6. In the window that opens, specify the file with the rule database.

   You can load only one archive containing an XML file with OVAL rules and XCCDF rules.

The total archive size must not exceed 2 MB.

7. Click **Open**.

   The **Source of rules** section displays information about the loaded rules. Follow the **Learn more** link in the **Platforms** field to open the window with the list of operating systems and products mentioned in the rules of the selected source.

8. If necessary, load the file with external variables:

   You cannot use external variables if the selected rule source contains XCCDF rules.

   a. Select the **Use external variables data with custom database** check box.

   b. Click the **Import external variables from file** link.

   c. In the window that opens, specify the path to the file with the external variables.

   d. Click **Open**.

9. In the **Scope** section, if necessary, change the vulnerability scan mode:

   The **Scope** section is unavailable if the selected rule source contains XCCDF rules.

   a. Select one of the modes:

   - **Scan all vulnerabilities**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the vulnerabilities database.

   - **Scan all vulnerabilities except added to the list**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect all vulnerabilities described in the rules of the vulnerabilities database except for those added to the list below.

   - **Scan vulnerabilities added to the list**.

     Kaspersky Industrial CyberSecurity for Nodes scans the devices to which the task is assigned in order to detect vulnerabilities added to the list below.

   b. If you selected **Scan all vulnerabilities except added to the list** or **Scan vulnerabilities added to the list**, create a list of vulnerabilities using the **Add** or **Add by conditions** buttons.

10. In the **Advanced settings** section, if necessary, determine the statuses of directive-based scans that will be included in the Security Audit task report:

    Directives cannot be applied if the selected rule source contains XCCDF rules.

    a. Select the **Use Directives** check box.

b. Using the switch next to each directive, determine the statuses of directive-based scans that will be displayed in the Security Audit task report.

If the switch next to a directive status is on, results of scans based on the directive's rules that have this status will be displayed in the Security Audit task report.

By default, the check boxes next to the **True** and **False** scan results are selected for all directives.

11. In the **Advanced settings** section, if necessary, configure settings for logging task completion events:

a. Select the **Enable logging** check box.

b. Select the desired **Logging level** from the list.

By default, the log is stored in the C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs folder.

The following logging levels are available:

- **Critical level** – only Critical events
- **Warning level** – only Critical and Warning events
- **Information level** – all Critical, Warning and Information events
- **Debug level** – all Critical, Warning, Information and Debug events

12. Click the **Save** button to save the task settings.

Viewing the Security Audit task execution results

To view the Security Audit task execution results:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the task name.
3. Select the **Application settings** tab.
4. Select the **Reports** section.

The list of reports contains task execution results sorted by date. Each line of the list contains the **task execution status** on the node specified in the task settings and the date and time when the task execution is completed.

Kaspersky Industrial CyberSecurity for Nodes returns the Security Audit task execution result:

- *Passed*.

  The Security Audit task gets this status if the scan result for the **Vulnerability** directive is *False* and for the remaining directives is *True*.

- *Not Passed*.

  The Security Audit task gets this status if the scan result for the **Vulnerability** directive is *True*, and for the remaining directives is *False*.

- *Warning*.

  The Security Audit task gets this status if the scan result for all directives is *Error*.

- *Other*.

  The Security Audit task gets this status if the scan result for all directives is *Unknown*, *Not evaluated*, or *Not applicable*.

You can filter the data in the report using filters.

The report on the Security Audit task execution results can be viewed in Kaspersky Security Center for 7 days after the task is completed, or until the task is removed.

Exporting the Security Audit task execution results to a separate file

To export the Security Audit task execution results to a separate file:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
2. Open the task settings window by clicking the task name.
3. Select the **Application settings** tab.
4. On the **Report** tab, select the desired report and click the **Details** button.
5. In the **Security audit results** window that opens, perform one of the following actions:

   - To receive an archive with a report on all task execution results in XML format, click **Export**.

     A ZIP archive with the report in XML format will be saved to the standard operating system folder for the downloaded files. If the task settings enabled logging security audit events, a ZIP archive with a log in TXT format is also added.

   - To receive an archive with the report on the task execution results in HTML format:

     a. If necessary, filter the report data using the **Filter** button.

     b. Click **Create report**.

     A ZIP archive with the report in HTML format will be saved to the standard operating system folder for the downloaded files. The report will include only the lines that match the filter.

   The name of the archive with the report contains the name of the node for which the task was executed, as well as the date and time when the task was executed.

Creating a thumbprint for the certificate for signing files with OVAL or XCCDF rules

To create a thumbprint for the certificate for signing files with OVAL or XCCDF rules:

1. On the device, run a command line interpreter (for example, Command Prompt `cmd.exe`) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the ovaldbmgr.exe file is located.

   By default, the file is located in the \tools\ovaldbmgr folder of the distribution kit.
3. Depending on the location of the certificate, run one of the following commands and press Enter:

   - To create a certificate and then place it the System Storage Local Machine:

     ```
     ovaldbmgr.exe --signer=make-cert --subject=<certificate name>
     ```

   - To create a certificate and then place it in the PFX container:

     ```
     ovaldbmgr.exe --signer=make-cert --subject=<certificate_name> --export --pwd=
     <password_for_accessing_the_PFX_container> --pfx=<full_path_and_file_name_of_the_PFX_container>
     ```

   If the certificate was created successfully, the thumbprint of the certificate will be returned in the command line.

Creating a Kaspersky Security Center installation package with custom OVAL or XCCDF rules

To create a Kaspersky Security Center installation package with OVAL or XCCDF rules as a signed archive:

1. On the device, run a command line interpreter (for example, Command Prompt `cmd.exe`) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the ovaldbmgr.exe file is located.

   By default, the file is located in the \tools\ovaldbmgr folder of the distribution kit.
3. Depending on the location of the signature certificate for the OVAL- or XCCDF-rules file, run one of the following commands:

   - If the signing certificate is located in System Storage Local Machine:

     ```
     ovaldbmgr.exe --make-package --command={replace|merge} --subject=<certificate name> --output=<full path> --
     source=<full path> <full path to the file with OVAL or XCCDF rules>
     ```

- If the signing certificate is located in the PFX container:

```
ovaldbmgr.exe --make-package --command={replace|merge} --pfx=<full path to the PFX container> --pwd=
<password to access the PFX container> --output=<full path> --source=<full path> <full path to the file
with OVAL or XCCDF rules>
```

Command parameters for creating a Kaspersky Security Center installation package

Options	Description
`--make-package`	Required argument. Creates an archive with files.
`--command={replace|merge}`	Required argument. This parameter defines the package deployment mode in Kaspersky Security Center. Available values: • `replace` – replace the installation package in Kaspersky Security Center repository with the one being created. • `merge` – merge the installation package being created with the one that already exists in the Kaspersky Security Center repository. If the parameter value is not specified, the task ends with an error.
`--pfx=<full path to the PFX container>`	Required argument. Parameter specifies the full path to the PFX container with signature certificate footprint for the OVAL- or XCCDF-rules file.
`--pwd=<password to access the PFX container>`	Required argument. This parameter defines the password to access the PFX container.
`--subject=<certificate name>`	Required argument. This parameter passes the name of the certificate for signing. If the name of a non-existent certificate for signing is specified, the command ends with an error.
`--output=<full path>`	Required argument. This parameter specifies the full path to the folder where the installation package will be created as a result of running the command.
`--source=<full path>`	This parameter specifies the full path to the folder that contains the folder with OVAL and XCCDF rules that you want to include in the Kaspersky Security Center package.
`<full path to the file with OVAL or XCCDF rules>`	This parameter defines the full path to the files with OVAL or XCCDF rules in XML format that you want to include in the Kaspersky Security Center package. OVAL and XCCDF rules must be saved in UTF-8 without BOM. The file with OVAL or XCCDF rules must be located in a folder inside another folder. For example: C:\Users\UserName\Desktop\folder\subfolder\OvalRules.xml You can specify several parameter values separated by spaces. To specify files with OVAL or XCCDF rules, select one of the following options: • Set only the `--source=<full path>` argument. • Specify one or more space-separated `<full path to OVAL or XCCDF rules>` values. • Simultaneously set `--source=<full path>` and specify one or more space-separated `<full path to the file with OVAL or XCCDF rules>` values. If no `<full path to the file with OVAL or XCCDF rules>` values are specified, and `--source=<full path>` is not set, the task finishes with an error.

As a result of running the command, Kaspersky Industrial CyberSecurity for Nodes creates:

- An archive named package.zip in the folder specified by the value of the `--output=<full path>` parameter. The archive contains the following files:
  - One or more ZIP files for each of the custom files with OVAL or XCCDF rules. Each archive contains one XML file with rules as well as the signature file for that XML file.
  - The ovaldbmgr.kud file for deploying the Kaspersky Security Center package.
  - The ovaldbmgr.exe deployment utility.
- Signature thumbprint used to sign the package.zip archive.

  You can specify the thumbprint in the Security Audit task settings using the custom rule database from the Kaspersky Security Center repository as the rule source.

Using Kaspersky Security Gateway

The application is compatible with Kaspersky Security Gateway version 4.0 or later.

Kaspersky Security Gateway is designed to transmit from Kaspersky Security Center to the SCADA system the diagnostic information received from Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks, or from Kaspersky Industrial CyberSecurity for Networks directly. The information about the protection status of the industrial network and individual computers of the network is displayed on the screen of the SCADA system, letting the operator of the SCADA system to respond promptly to industrial network protection problems.

Kaspersky Security Gateway uses the following communication protocols to interact with SCADA systems:

- **IEC 60870-5-104**. Unified open protocol for automation systems.
- **OPC DA**. Device interaction specification for industrial networks based on the Microsoft COM technology.
- **OPC UA**. Device interaction specification for industrial networks that provides cross-platform compatibility.

You can configure data transfer settings either using the Kaspersky Security Gateway graphical user interface or standard Microsoft Windows tools.

Diagnostic information

Kaspersky Security Gateway transmits the following information to the SCADA system:

- **SecurityServerAvailable**. Availability of the Kaspersky Security Center Administration Server. Possible values:
  - `1` Kaspersky Security Gateway has successfully connected to the Kaspersky Security Center Administration Server.
  - `0` Kaspersky Security Gateway cannot connect to the Kaspersky Security Center Administration Server.
- **AllSecuredHostAvailable**. Availability of all protected computers on the network. A computer is available if a protection application and the Network Agent are running on it. Possible values:
  - `0` At least one computer managed by the Kaspersky Security Center Administration Server and selected for monitoring in Kaspersky Security Gateway settings is unavailable at the moment when the status is determined.
  - `1` All computers managed by the Kaspersky Security Center Administration Server and selected for monitoring in Kaspersky Security Gateway settings are available at the moment when the status is determined.

  If there is no connectivity between at least one computer and the Kaspersky Security Center Administration Server, the value of `0` (unavailable) is sent.

- **GeneralizedThreatOccured**. Protection status of the network. Possible values:
  - `0` No threats detected on all computers of the network.
  - `1` At least one computer on the network has a detected threat.
  - `2` At least one computer on the network has a warning.

  When determining the network protection status, the Kaspersky Security Gateway uses status information only for those computers that have been selected in the Kaspersky Security Gateway settings to be displayed in the SCADA system.
- **<Computer name>**. Availability and protection status of the computer. The computer is available a protection application and the Network Agent are running on it. Possible values:
  - `-1` Unable to retrieve the status of the computer.
  - `0` The computer is available.
  - `1` A threat has been detected on the computer.
  - `2` A warning has been issued for the computer.
  - `3` The computer is unavailable.

  Kaspersky Security Gateway sends status information only for those computers that have been selected in the Kaspersky Security Gateway settings to be displayed in the SCADA system.

  > If there is no connectivity between the computer or Kaspersky Security Gateway and the Kaspersky Security Center Administration Server, the value of `-1` (unable to retrieve the status of the computer) is sent.
- **<PLC name>**. Status of the PLC connected to Kaspersky Security Center:
  - `-1` Unable to retrieve the status.
  - `0` No error messages or PLC was not checked.
  - `1` Critical error (for example, PLC project does not match reference project).
  - `2` Warnings.
  - `3` PLC unavailable.
- **<Name of the device>**. Device status (PLC or IED) connected to Kaspersky Industrial CyberSecurity for Networks:
  - `-1` Unable to retrieve the status.
  - `0` No error messages or the device has not been checked.
  - `1` Critical error (for example, PLC project does not match reference project).

- `2` Warnings.
- `3` The device is unavailable.

- **UnauthorizedSystemCommandCount**. New event counter for a device connected to Kaspersky Industrial CyberSecurity for Networks. Possible values:
  - `<number>` Number of new events.
  - `-1` Unable to retrieve the status.

Limitations and known issues of Kaspersky Security Gateway

- To connect Kaspersky Security Gateway installed on the device running Windows 7, Windows Server 2008, or Windows Server 2012 to Kaspersky Security Center 14 and later, TLS 1.1 and 1.2 must be enabled in the operating system as default secure protocols. For details, please refer to the Microsoft documentation.
- The `gateway_service.exe` emergency termination may be caused by errors in the third-party grpc library. The service emergency termination occurs when connection to Kaspersky Industrial CyberSecurity for Networks is established at the same time when dynamic code analysis is performed using the Application Verifier utility.
- Kaspersky Security Gateway is compatible with Kaspersky Industrial CyberSecurity for Networks version 4.2 and later.
- When using the KSG OPC UA server together with PcVue 16.2, PcVue 16.2 may crash when the SessionsDiagnosticsSummary node is opened.
- When using the OPC DA and OPC UA protocols, tag values must be of the int type.
- The Quality tag status is not used and always has the GOOD value. When tracking for a tag is disabled, it is excluded from the transmitted data. Tag with a changed status (BAD or COM_FAILURE) cannot be transmitted.
- After Kaspersky Security Gateway starts, it does not transmit tag values to the SCADA system until it receives data from Kaspersky Security Center or Kaspersky Industrial CyberSecurity for Networks.

  Updating Kaspersky Security Gateway from version 4.5 or earlier to 5.0 disables trace file logging. If necessary, configure trace file logging again.
- If a monitored device has been removed from Kaspersky Industrial CyberSecurity for Networks, that device will no longer appear in the **Tracked data** section of the Kaspersky Security Gateway Console; however, tags with the value `-1` for **<Device name>** and a value of `0` for **UnauthorizedSystemCommandCount** will continue to be transmitted for that device. To stop sending data about a remote device:

  1. Open the Kaspersky Security Gateway Console
  2. In the **Kaspersky Security Gateway** node, select the protocol used.
  3. In the results pane, under **Tracked data**, click the **Change** link.

     The **Selecting tracked data** window opens.
  4. No changes are required; close the window by clicking **OK**.

Kaspersky Security Gateway Console interface

Kaspersky Security Gateway Console is displayed in the Microsoft Management Console tree in the form of a node with the name **Kaspersky Security Gateway**.

The Console tree displays a **Kaspersky Security Gateway** node and child nodes for configuring data transfer protocols to be used in the SCADA system:

- **IEC 60870-5-104**.
- **OPC DA**.
- **OPC UA**.

The results pane of the **Kaspersky Security Gateway** node displays:

- General information about Kaspersky Security Gateway.
- Detailed information about the settings for connecting to Kaspersky Security Center and Kaspersky Industrial CyberSecurity for Networks, and a link to the settings window.
- Details about current Kaspersky Security Gateway additional settings and a link to the settings window.

Configuring a connection with Kaspersky Security Center

To configure a connection to Kaspersky Security Center:

1. Open the Kaspersky Security Gateway Console
2. Select the **Kaspersky Security Gateway** node.
3. In the **Connection Settings** section of the results pane, click the **Configure connection** link.

   The **Connection Settings** window opens.
4. Under **Kaspersky Security Center**, specify settings for connecting to the Kaspersky Security Center Administration server:

   - **Server**. IP address or domain name of the Kaspersky Security Center Administration Server and the number of the port used to connect to it. For detailed information on configuring the connection to the Administration Server, see Kaspersky Security Center Help. Range of possible values for the port number: 1–65535.
   - **User name**. Account name of the administrator of the Kaspersky Security Center Administration Server.
   - **Password**. Account password of the administrator of the Kaspersky Security Center Administration Server.

5. Select the connection type:

- **Disabled**. The connection to the Kaspersky Security Center administration server cannot be established.
- **Open API**. If the Open API interface is selected as the data provider, you must **export the Kaspersky Security Center root certificate** and install it in the Certificate store of trusted root certificate authorities (CA). For the Open API data provider, the default port number is 13299.

  1. In the browser, enter `https://<Web Console address>:13299`.
  2. In your browser, open the certificate information for the established connection with the Kaspersky Security Center Web Console.
  3. In the **Certificates** window, select the **Certificate path** tab.
  4. Select the root certificate.
  5. Go to the **Details** tab.
  6. Export the selected certificate by clicking the **Copy to file** button.

- **klakaut**. The *klakaut* is the Kaspersky Security Center Automation utility, which lets you manage Kaspersky Security Center Administration Server via the external API using COM (Component Object Model) objects. If the klakaut utility is selected as the data provider, you must install the Kaspersky Security Center Administration Console before installing Kaspersky Security Gateway on the same computer. For the Klakaut data provider, the default port number is 13291. This option is selected by default.

  If you install Kaspersky Security Center Administration Console after Kaspersky Security Gateway, the connection between Kaspersky Security Gateway and the Kaspersky Security Center Administration Server cannot be established.

- **Automatically**. The application attempts to connect to the Kaspersky Security Center Administration Server using klakaut and Open API. This option is selected by default after updating Kaspersky Security Gateway version 4.5 or earlier to version 5.0.

  The **Automatic** connection type is available only after installing a new version of Kaspersky Security Gateway over the previous one. Once you change the connection type, this option will no longer appear in the drop-down list.

6. Click the **Connection scan** button.

   The status *Connected* appears when the connection is established.

7. Click **OK**.

8. Click the **OK** button to close the **Kaspersky Security Gateway** window.

You can also configure connection settings using the `ConnectionSettings.xml` configuration file located in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder. Note that you cannot set the password in the configuration file. Use Kaspersky Security Gateway Console to set the password.

Configuring a connection with Kaspersky Industrial CyberSecurity for Networks

To configure connection with Kaspersky Industrial CyberSecurity for Networks

1. Open the Kaspersky Security Gateway Console
2. Select the **Kaspersky Security Gateway** node.
3. In the **Connection Settings** section of the results pane, click the **Configure connection** link.

   The **Connection Settings** window opens.
4. Under **Kaspersky Industrial CyberSecurity for Networks**, add connection settings for one or more Kaspersky Industrial CyberSecurity for Networks servers:

   a. Click the **Add** button.

   The **Kaspersky Industrial CyberSecurity for Networks connection settings** window opens.

   b. Enter the IP address of the Generic type connector previously added to Kaspersky Industrial CyberSecurity for Networks, along with the port number used to connect to it. Range of possible values for the port number: 1–65535.

   > Connector connection settings differ from the connection settings of the Kaspersky Industrial CyberSecurity for Networks integration server. For detailed information on connectors, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

   c. If you want to configure a trusted connection with Kaspersky Industrial CyberSecurity for Networks:

      1. Select the **Use pinned certificate to secure connection** check box.
      2. Click **Load**.
      3. This opens a window; in that window, select the file with the TLS certificate.
      4. Click **Open**.

      Information about the added TLS certificate is displayed under **TLS certificate data**.

      > If you specified a pinned certificate to protect the connection, you must also specify the client certificate. Otherwise, the connection with the Kaspersky Industrial CyberSecurity for Networks cannot be established.

   d. If you want to configure additional protection of the connection using a client certificate:

      1. Select the **Secure connection with client certificate** check box.
      2. Click **Load**.

3. This opens a window; in that window, select a PFX file with the client certificate.

4. Click **Open**.

5. In the field with the same name, enter the password of the client certificate, if any.

e. Click **Test connection**.

The status *Connected* appears when the connection is established.

f. Click **OK**.

g. If necessary, repeat steps a–f to add connection settings for other Kaspersky Industrial CyberSecurity for Networks servers.

Kaspersky Industrial CyberSecurity for Networks connection information is displayed in the list in the **Connection settings** window.

5. Click **OK**.

You can also configure connection settings using the `ConnectionSettings.xml` configuration file located in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder. Note that you cannot set the password in the configuration file. Use Kaspersky Security Gateway Console to set the password.

Configuring the DCOM protocol

If the computers involved in sending and receiving data via the OPC DA protocol are not joined to an Active Directory domain, create user accounts with the same name and password for each of these computers.

To establish an OPC DA connection, configure access permissions for the Distributed Component Object Model (DCOM) protocol.

How to configure the DCOM protocol for interaction between Kaspersky Security Gateway and SCADA-system installed on one computer

1. On the computer with Kaspersky Security Gateway and SCADA-system installed, between which you want to configure interaction, press the **Win+R** key combination.

   The standard Microsoft Window **Run** window opens.

2. Enter *dcomcnfg* in the **Open** field and press **OK**.

   The **Component Services** window opens.

3. In the left part of the window, in the folder tree, select **Component Services** → **Computers** → **My Computer**.

4. Open the context menu of the **My Computer** folder and select **Properties**.

5. Select the **COM Security** tab in the **My Computer Properties** window.

6. Under **Access Permissions**, click **Edit Default**.

   This opens the **Access Permission** window.

7. Under **Group or user names**, select the **NETWORK SERVICE** group.

8. In the table of permissions for the **NETWORK SERVICE** group, in the **Allow** column, select the **Local Access** and **Remote Access** check boxes.

9. Select the **Default Properties** tab and make sure that the following values are configured: **Default Authentication Level –** *Connect*, **Default Impersonation Level** – *Identify*.

10. Click **OK**.

11. Click the **OK** button in the **Properties: My Computer** window.

12. Restart the computer.

How to configure the DCOM protocol for interaction between Kaspersky Security Gateway and SCADA-system installed on different computers

On both computers:

1. Press the **`Win+R`** key combination.

   The standard Microsoft Window **Run** window opens.

2. Enter *dcomcnfg* in the **Open** field and press **OK**.

   The **Component Services** window opens.

3. In the left part of the window, in the folder tree, select **Component Services** → **Computers** → **My Computer**.

4. Open the context menu of the **My Computer** folder and select **Properties**.

5. Select the **COM Security** tab in the **My Computer Properties** window.

6. In the **Access Permission** section, click the **Edit Limits** button.

   This opens the **Access Permission** window.

7. In the **Group or user names** section, select the **ANONYMOUS LOGON** group.

8. In the table of permissions for the **ANONYMOUS LOGON** group, in the **Allow** column, select the **Local Access** and **Remote Access** check boxes.

   > Allowing remote access to the ANONYMOUS LOGON group affects the security level of the system. We recommend testing the functioning of the OPC DA protocol without this permission and grant the permission only if working without it is impossible.

9. Under **Access Permissions**, click **Edit Default** and retrace steps 7 through 8 of the instructions.

10. Under **Launch and Activation Permissions**, click **Edit Limits** and retrace steps 7 through 8 of the instructions.

11. Under **Launch and Activation Permissions**, click **Edit Default** and retrace steps 7 through 8 of the instructions.

12. On the **Default Properties** tab, make sure that the following values are configured: **Default Authentication Level –** *Connect*, **Default Impersonation Level** – *Identify*.

13. Click **OK**.

14. Click the **OK** button in the **Properties: My Computer** window.

15. Configure the OPCEnum application.

    a. In the left part of the window, in the folder tree, select **Component Services** → **Computers** → **My Computer** → **DCOM Config** → **OPCEnum**.

    b. Right-click to bring up the context menu of **OPCEnum** and select **Properties**.

    This opens the **Properties: OPCEnum** window.

    c. On the **General** tab, make sure that **Default Authentication Level** is set to *Connect*.

    d. On the **Security** tab, under **Launch and Activation Permissions**, click **Edit**.

    e. Under **Group or user names**, select the **All** group.

    f. In the permission table of the **All** group, in the **Allow** column, select the **Local Access**, **Remote Access**, **Local Activation**, **Remote Activation** check boxes.

    g. Under **Access Permissions** section, click the **Edit** button.

    h. Under **Group or user names**, select the **All** group.

    i. In the table of permissions for the **All** group, in the **Allow** column, select the **Local Access** and **Remote Access** check boxes.

    j. On the **Identity** tab, select **The system account**.

    k. Click **OK**.

16. Restart the computer.

On the computer where the Kaspersky Security Gateway utility is installed:

1. Press the **Win+R** key combination.

   The standard Microsoft Window **Run** window opens.

2. Enter *dcomcnfg* in the **Open** field and press **OK**.

   The **Component Services** window opens.

3. In the left part of the window, in the folder tree, select **Component Services** → **Computers** → **My Computer** → **DCOM Config** → **Kaspersky Gateway OPC Service**.

4. Open the context menu of **Kaspersky Gateway OPC Service** and select **Properties**.

   This opens the **Properties: Kaspersky Gateway OPC Service** window.

5. On the **General** tab, make sure that **Default Authentication Level** is set to *Connect*.

6. Click **OK**.

7. If Kaspersky Security Gateway and the SCADA system are installed on computers that belong to different domains:

   a. In the operating system, open **Control Panel** – **Administrative Tools** – **Local Security Policy**.

   b. In the local security policy console tree, select the **Local Policies** – **Security Options** section.

   c. In the workspace of the **Security Options** section, in the context menu of the **Network access: Let Everyone permissions apply to anonymous users** local policy, select **Enabled**.

8. Restart the computer.

Configuring data transfer settings using communication protocols

This section provides instructions on configuring data transfer using available communication protocols.

Configuring data transfer using IEC 60870-5-104 protocol

To configure data transfer via the IEC 60870-5-104 protocol using the Kaspersky Security Gateway Console:

1. Open the Kaspersky Security Gateway Console
2. In the **Kaspersky Security Gateway** node select **IEC 60870-5-104**.
3. In the **Data transmission settings** section in the results pane, click the **Change** link.

   The **Settings** window opens.
4. In the **Transmission settings** section, disable or enable the **Enable data transmission** option.

   If this functionality is enabled, Kaspersky Security Gateway sends the protection status of the industrial network nodes to the SCADA system. By default, the functionality is disabled.
5. In the **Connection settings** group box configure the following:

   - **Device address**. An auxiliary address assigned to the computer in the SCADA system. Range of possible values: 1–65535.
   - **Device port**. A port number for establishing a connection to the SCADA system. Range of possible values: 1–65535.
   - **TCP connection timeout**. The value is specified in seconds. Range of possible values: 1–255.
   - **Message send timeout**. The value is specified in seconds. Range of possible values: 1–255.
   - **Message confirmation timeout**. The value is specified in seconds. Range of possible values: 1–255.
   - **Test connection timeout**. The value is specified in seconds. Range of possible values: 1–255.

- **Maximum unconfirmed received messages allowed**. Range of possible values: 1–32767.
- **Maximum unconfirmed sent messages allowed**. Range of possible values: 1–32767.

6. Click **OK**.
7. In the **Tracked data** section in the results pane, click the **Change** link.

   The **Selecting tracked data** window opens. The list displays tracked data added automatically after connecting to a data source, such as Kaspersky Security Center and/or Kaspersky Industrial CyberSecurity for Networks.
8. Select or clear check boxes next to the names of computers to enable or disable the tracking of their availability and protection status. The computer is available a protection application and the Network Agent are running on it.

   If tracking is enabled, data will be transmitted to the SCADA system.

   If tracking is disabled, data will not be transmitted to the SCADA system.

   > If there is no connectivity between the computer or Kaspersky Security Gateway and the Kaspersky Security Center Administration Server, the value of `-1` (unable to retrieve the status of the computer) is sent.
9. If required, edit or add a service tag in the **Service tag** column. You can use the service tag to filter data received in the SCADA system. The tag may consist of numbers only.
10. Click **OK**.

You can configure data transfer over the IEC 60870-5-104 protocol using the `ProtocolEICSettings.xml` configuration file in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder.

Configuring data transfer using OPC DA protocol

The following prerequisites must be met to successfully transfer data via the OPC DA protocol:

- The required DCOM rights are assigned to OPCEnum both on the SCADA system and in Kaspersky Security Gateway.
- Unified authentication is set for the computer with Kaspersky Security Gateway installed and the SCADA system: domain authentication is used, or the same user name / password are used for all computers of the work group.

To configure data transfer via the OPC DA protocol using the Kaspersky Security Gateway Console:

1. Open the Kaspersky Security Gateway Console
2. In the **Kaspersky Security Gateway** node select **OPC DA**.
3. In the **Data transmission settings** section in the results pane, click the **Change** link.

   The **Settings** window opens.

4. Disable or enable the **Enable data transmission** option.

   If this functionality is enabled, Kaspersky Security Gateway sends the protection status of the industrial network nodes to the SCADA system. By default, the functionality is disabled.

5. Click **OK**.

6. In the **Tracked data** section in the results pane, click the **Change** link.

   The **Selecting tracked data** window opens. The list displays tracked data added automatically after connecting to a data source, such as Kaspersky Security Center and/or Kaspersky Industrial CyberSecurity for Networks.

7. Select or clear check boxes next to the names of computers to enable or disable the tracking of their availability and protection status. The computer is available a protection application and the Network Agent are running on it.

   If tracking is enabled, data will be transmitted to the SCADA system.

   If tracking is disabled, data will not be transmitted to the SCADA system.

   > If there is no connectivity between the computer or Kaspersky Security Gateway and the Kaspersky Security Center Administration Server, the value of `-1` (unable to retrieve the status of the computer) is sent.

8. If required, edit or add a service tag in the **Service tag** column. You can use the service tag to filter data received in the SCADA system. A tag may contain numbers or letters.

9. Click **OK**.

You can configure data transfer over the OPC DA protocol using the `ProtocolOPCSettings.xml` configuration file in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder.

Configuring data transfer using OPC UA protocol

To configure data transfer via the OPC UA protocol using the Kaspersky Security Gateway Console:

1. Open the Kaspersky Security Gateway Console

2. In the **Kaspersky Security Gateway** node select **OPC UA**.

3. In the **Data transmission settings** section in the results pane, click the **Change** link.

   The **Settings** window opens.

4. Disable or enable the **Enable data transmission** option.

   If this functionality is enabled, Kaspersky Security Gateway sends the protection status of the industrial network nodes to the SCADA system. By default, the functionality is disabled.

5. Under **Connection settings**, enter the port number for establishing a connection to the SCADA system. Range of possible values for the port number: 1–65535.

6. Click **OK**.

7. In the **Tracked data** section in the results pane, click the **Change** link.

   The **Selecting tracked data** window opens. The list displays tracked data added automatically after connecting to a data source, such as Kaspersky Security Center and/or Kaspersky Industrial CyberSecurity for Networks.

8. Select or clear check boxes next to the names of computers to enable or disable the tracking of their availability and protection status. The computer is available a protection application and the Network Agent are running on it.

   If tracking is enabled, data will be transmitted to the SCADA system.

   If tracking is disabled, data will not be transmitted to the SCADA system.

   > If there is no connectivity between the computer or Kaspersky Security Gateway and the Kaspersky Security Center Administration Server, the value of `-1` (unable to retrieve the status of the computer) is sent.

9. If required, edit or add a service tag in the **Service tag** column. You can use the service tag to filter data received in the SCADA system. A tag may contain numbers or letters.

10. Click **OK**.

You can configure data transfer over the OPC UA protocol using the `ProtocolOPCUASettings.xml` configuration file in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder.

Configuring data transfer using a configuration file

Editing configuration files requires specialist knowledge. Incorrectly editing configuration files may cause Kaspersky Security Gateway errors.

To configure data transfer using a configuration file:

1. In any text editor, open the configuration file with the Kaspersky Security Gateway settings in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder:

   - `ProtocolIECSettings.xml` is the configuration file for the IEC 60870-5-104 protocol.
   - `ProtocolOPCSettings.xml` is the configuration file for the OPC DA protocol.
   - `ProtocolOPCUASettings.xml` is the configuration file for the OPC UA protocol.

2. Configure data transfer settings.

3. Save the configuration file.

4. Restart Kaspersky Security Gateway service to apply the new settings.

Configuring Kaspersky Security Gateway additional settings

To configure additional settings of Kaspersky Security Gateway:

1. Open the Kaspersky Security Gateway Console
2. Select the **Kaspersky Security Gateway** node.
3. In the **Application Settings** section of the results pane, click the **Configure application settings** link.
   The **Application settings** window opens.
4. In the **Interrogation** section, set the **Interrogation period (sec)**.
5. In the **System tracing** section:
   - Clear or select the **Enable tracing** check box.
   - In the drop-down list, select the **Level** of information to be logged.
6. In the **Application settings** window, click **OK**.

You can configure the advanced settings of Kaspersky Security Gateway using the `AppSettings.xml` configuration file in the `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` folder.

Viewing Kaspersky Security Gateway events

The following events can occur during the operation of Kaspersky Security Gateway:

- Enabling and disabling of the Kaspersky Security Gateway service.
- Communication problems between Kaspersky Security Gateway and the SCADA system.
- Problems connecting to the Kaspersky Security Center Administration Server and receiving data from the Administration Server.
- Problems accessing the Kaspersky Security Gateway configuration file.

Information about such events is recorded in trace files that are stored in the `%ProgramData%\Kaspersky Lab\Security Gateway\Traces` folder.

BitLocker Full Disk Encryption management

BitLocker is an encryption technology built into Windows operating systems. Kaspersky Industrial CyberSecurity for Nodes allows you to control and manage Bitlocker using Kaspersky Security Center. BitLocker encrypts logical volumes. For more details on BitLocker, refer to the Microsoft documentation.

Kaspersky Industrial CyberSecurity for Nodes does not support managing BitLocker on Windows Vista and Windows Server 2008 computers.

When encrypting the disk, BitLocker puts the boot loader and other auxiliary files in the system partition. This partition is not encrypted. The operating system creates the system partition automatically during the installation of Windows. If the disk is fully partitioned before installing Windows, the operating system cannot create a system partition. In this case, when you start BitLocker disk encryption, the operating system prompts you to repartition the disk and create a system partition. After creating a system partition, the operating system starts BitLocker encryption.

Kaspersky Industrial CyberSecurity for Nodes does not support BitLocker encryption of removable drives.

BitLocker provides secure storage of access keys by using a trusted platform module. A *Trusted Platform Module* (TPM) is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus. Using TPM is the safest way to store BitLocker access keys, since TPM provides pre-startup system integrity verification. You can still encrypt drives on a computer without a TPM. In this case, the access key will be encrypted with a password. BitLocker uses the following authentication methods:

- TPM.
- TPM and PIN.
- Password.

Before encrypting a drive, BitLocker creates a recovery key. Kaspersky Industrial CyberSecurity for Nodes reads and sends the recovery key to Kaspersky Security Center, allowing you to restore access to the disk, for example, if a user has forgotten the password.

After encrypting the system hard drive, the user needs to go through BitLocker authentication to boot the operating system. After authentication, BitLocker allows the user to log in. BitLocker does not support single sign-on technology (SSO).

If a user encrypts a disk using BitLocker, Kaspersky Industrial CyberSecurity for Nodes will send information about disk encryption and the recovery key to Kaspersky Security Center.

If you are using Windows group policies, turn off BitLocker management in the policy settings. Windows policy settings may conflict with Kaspersky Industrial CyberSecurity for Nodes policy settings. When encrypting a drive, errors may occur.

Starting BitLocker Drive Encryption

Prior to starting full disk encryption, you are advised to make sure that the computer is not infected. To do so, start the Full Scan or Critical Areas Scan task. Performing full disk encryption on a computer that is infected by a rootkit may cause the computer to become inoperable.

To use BitLocker Drive Encryption on computers running Windows operating systems for servers, installing the BitLocker Drive Encryption component may be required. Install the component using the operating system tools (Add Roles and Components Wizard). For more information about installing BitLocker Drive Encryption, refer to the Microsoft documentation.

How to run BitLocker Drive Encryption in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Data Encryption** section.
4. In the **Encryption mode** drop-down list, select **Encrypt all hard drives**.

   If the computer has several operating systems installed, after encryption you will be able to load only the operating system in which the encryption was performed.

5. Configure advanced BitLocker Drive Encryption options (see table below).
6. Click **OK** to save the changes.

How to run BitLocker Drive Encryption in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Data Encryption** section.
5. Click the **Configure** button in the **Full Disk Encryption** subsection.
6. In the **Encryption mode** drop-down list, select **Encrypt all hard drives**.

   If the computer has several operating systems installed, after encryption you will be able to load only the operating system in which the encryption was performed.

7. Configure advanced BitLocker Drive Encryption options (see table below).

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

You can use the Application Console to control the disk encryption or decryption process on a user computer.

After applying a policy, depending on the authentication settings, the application displays the following requests in the Compact Diagnostic Interface window or the Application Console:

- TPM only. No user input required. The disk will be encrypted when the computer restarts.
- TPM + PIN / Password. If a TPM module is available, a PIN code prompt window appears. If a TPM module is not available, you will see a password prompt window for preboot authentication.
- Password only. You will see a password prompt window for preboot authentication.

If the Federal Information Processing standard compatibility mode is enabled for computer operating system, then in Windows 8 and earlier versions of operating system, a request for connecting a storage device is displayed to save the recovery key file. You can save multiple recovery key files on a single storage device.

After setting a password or a PIN code, BitLocker prompts for a restart of the user's computer to check the compatibility of the computer with BitLocker. Kaspersky Industrial CyberSecurity for Nodes displays a corresponding notification in the Compact Diagnostic Interface window or the Application Console. Next, the user needs to go through the BitLocker authentication procedure. After the authentication procedure, the user must log on to the system. After the operating system has loaded, BitLocker starts the encryption.

If there is no access to encryption keys, the user may request the local network administrator to provide a recovery key (if the recovery key was not saved earlier on the storage device or was lost).

BitLocker Drive Encryption component settings

Parameter	Description
Enable use of BitLocker authentication requiring pre-boot keyboard input on tablets	Using authentication that requires data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets). The touchscreen of tablet computers is not available in the preboot environment. To complete BitLocker authentication on tablet computers, the user must connect a USB keyboard, for example. If the check box is selected, use of authentication requiring preboot input is allowed. We recommend using this setting only for devices that have alternative data input tools in a preboot environment, such as a USB keyboard in addition to touchscreen keyboards. If the check box is cleared, BitLocker Drive Encryption is not possible on tablets.
Use hardware encryption (Windows 8 and later versions)	If the check box is selected, the application applies hardware encryption. This lets you increase the speed of encryption and use fewer computer resources.
Encrypt used disk space only (Windows 8 and later versions)	This check box enables / disables the option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time. Enabling or disabling the **Encrypt used disk space only (Windows 8 and later versions)** feature after starting encryption does not modify this setting until the hard drives are decrypted. You must select or clear the check box before starting encryption. If the check box is selected, only portions of the hard drive that are occupied by files are encrypted. Kaspersky Industrial CyberSecurity for Nodes encrypts new data automatically as they are added. If the check box is cleared, the entire hard drive is encrypted, including residual fragments of previously deleted and modified files. This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable. By default, the check box is cleared.

Parameter	Description
Authentication method	**Trusted platform module (TPM)** If this option is selected, BitLocker uses a Trusted Platform Module (TPM). A Trusted Platform Module (TPM) is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus. For computers running Windows 7 or Windows Server 2008 R2, only encryption using a TPM module is available. If a TPM module is not installed, BitLocker encryption is not possible. Use of a password on these computers is not supported. A device equipped with a Trusted Platform Module can create encryption keys that can be decrypted only with the device. A Trusted Platform Module encrypts encryption keys with its own root storage key. The root storage key is stored within the Trusted Platform Module. This provides an additional level of protection against attempts to hack encryption keys. This action is selected by default. You can set an additional layer of protection for access to the encryption key, and encrypt the key with a password or a PIN: **Use PIN for TPM**. If this check box is selected, a user can use a PIN code to obtain access to an encryption key that is stored in a Trusted Platform Module (TPM). If this check box is cleared, users are prohibited from using PIN codes. To access the encryption key, a user must enter the password. **Trusted platform module (TPM), or password if TPM is unavailable** If this option is selected, the user can use a password to obtain access to encryption keys when a Trusted Platform Module (TPM) is not available. If the check box is cleared and the TPM is not available, full disk encryption will not start. **Only password (Windows 8 and later versions)** If this option is selected, Kaspersky Industrial CyberSecurity for Nodes prompts the user for a password when the user attempts to access an encrypted drive. This option can be selected when a Trusted Platform Module (TPM) is not being used. The selected authentication method must be configured by specifying password or PIN requirements: • **Minimum PIN length (characters)**. • **Use enhanced PIN (letters and numbers)**. Enhanced PIN allows using other characters in addition to numerical characters: uppercase and lowercase Latin letters, special characters, and spaces. • **Minimum password length (characters)**. • **Limit password / PIN validity period for TPM (days)**.
Automatically recreate recovery key (days)	Automatically update the password to restore access to a drive protected by BitLocker. If the check box is selected, specify the validity period of the recovery key password.

Decrypting a hard drive protected by BitLocker

Users can decrypt a disk using the operating system (the *Turn Off BitLocker* function). After this, Kaspersky Industrial CyberSecurity for Nodes prompts to re-encrypt the disk. Kaspersky Industrial CyberSecurity for Nodes will be prompting to encrypt the disk unless you enable disk decryption in the policy.

How to decrypt a hard drive protected by BitLocker using the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Data Encryption** section.
4. In the **Encryption mode** drop-down list, select **Decrypt all hard drives**.
5. Click **OK** to save the changes.

How to decrypt a hard drive protected by BitLocker using the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Data Encryption** section.
5. Click the **Configure** button in the **Full Disk Encryption** subsection.
6. In the **Encryption mode** drop-down list, select **Decrypt all hard drives**.
7. Click **OK** to save the changes.

You can use the Application Console to control the disk encryption or decryption process.

Restoring access to a drive protected by BitLocker

If a user has forgotten the password for accessing a hard drive encrypted by BitLocker, you need to start the recovery procedure (Request-Response).

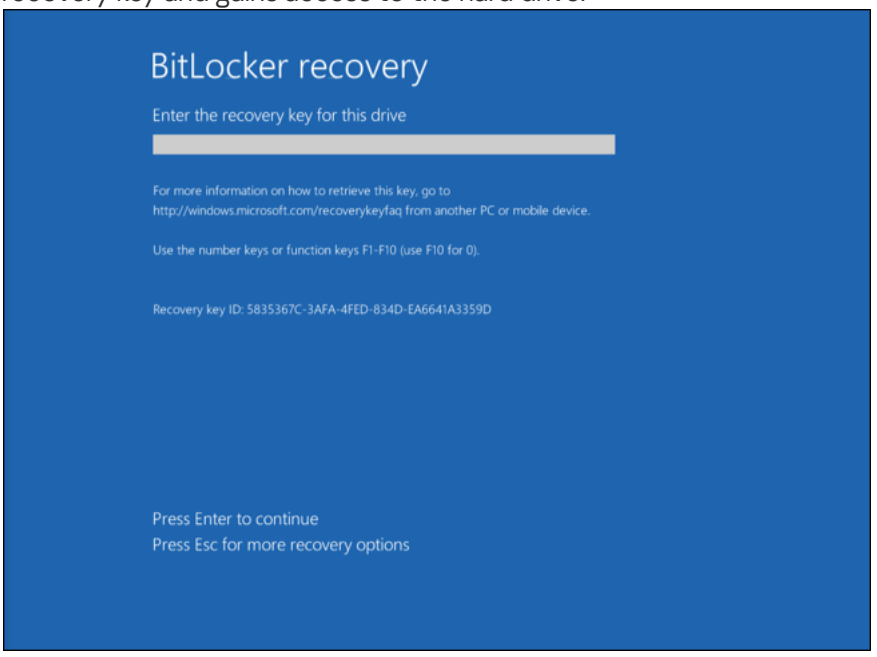
If the computer's operating system has Federal Information Processing standard (FIPS) compatibility mode enabled, then in Windows 8 and older the recovery key file is saved to the removable drive before encryption. To restore access to the drive, insert the removable drive and follow the on-screen instructions.

Restoring access to a hard drive encrypted by BitLocker consists of the following steps:

1. The user tells the administrator the recovery key ID (see the figure below).
2. The administrator verifies the ID of the recovery key in the computer properties in Kaspersky Security Center. The ID that the user provided must match the ID that is displayed in the computer properties.

   If the recovery key IDs match, the administrator hands over the recovery key to the user.

3. The user enters the recovery key and gains access to the hard drive.



Restoring access to a hard drive encrypted by BitLocker

Restoring access to a system drive

To start the recovery procedure, the user needs to press the **Esc** key at the pre-boot authentication stage.

How to view the recovery key for a system drive encrypted by BitLocker in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Managed devices**.
2. Go to the **Devices** tab.
3. Open the context menu of the user computer that requested encrypted data access recovery.
4. In the context menu, select **Grant access in offline mode**.
5. Ask the user for the recovery key ID indicated in the BitLocker password input window, and compare it with the ID in the **Recovery key ID** field on the **Access to a BitLocker-protected system drive** tab.

   If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

6. Send the user the key that is indicated in the **Recovery key** field.

How to view the recovery key for a system drive encrypted by BitLocker in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
2. Select the check box next to the name of the computer whose drive you want to restore access to.
3. Click **Grant access to the device in offline mode**.

4. Verify the recovery key ID. The ID provided by the user must match the ID that is displayed in the computer settings.

   If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

5. Click **Receive key**.

6. Send the user the key that is indicated in the **Recovery key** field.

After the operating system is loaded, Kaspersky Industrial CyberSecurity for Nodes prompts the user to change the password or PIN code. After you set a new password or PIN code, BitLocker creates a new recovery password, which the application sends to Kaspersky Security Center.

Restoring access to a non-system drive

To start the recovery procedure, the user needs to click the **Forgot your password** link in the window providing access to the drive. After gaining access to the encrypted drive, the user can enable automatic unlocking of the drive during Windows authentication in the BitLocker settings.

How to view the recovery key for a non-system drive encrypted by BitLocker in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select the **Advanced** → **Data encryption and protection** → **Encrypted drives** folder.

2. In the workspace, select the encrypted device for which you want to create an access key file, then in the context menu of the device, click **Get access to the device in Kaspersky Industrial CyberSecurity for Nodes**.

3. Prompt the user for the recovery key ID indicated in the BitLocker password input window, and compare it with the ID in the **Recovery key ID** field.

   If the IDs do not match, this key is not valid for restoring access to the specified drive. Make sure that the name of the selected computer matches the name of the user's computer.

4. Send the user the key that is indicated in the **Recovery key** field.

How to view the recovery key for a non-system drive encrypted by BitLocker in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Operations** → **Data encryption and protection** → **Encrypted drives**.

2. Select the check box next to the name of the computer whose drive you want to restore access to.

3. Click **Grant access to the device in offline mode**.

   This starts the Wizard for granting access to a device.

4. Follow the instructions of the Wizard for granting access to a device:

   a. Select the Kaspersky Industrial CyberSecurity for Nodes plug-in.

   b. Verify the recovery key ID. The ID provided by the user must match the ID that is displayed in the computer settings.

      If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

   c. Click **Receive key**.

5. Send the user the key that is indicated in the **Recovery key** field.

Pausing BitLocker protection to update software

There are a number of special considerations for updating the operating system, installing update packages for the operating system, or updating other software with BitLocker protection turned on. Installing updates may require restarting the computer multiple times. After each restart, the user must complete BitLocker authentication. To make sure updates install correctly, you can temporarily turn off BitLocker authentication. In this case the disk stays encrypted and the user has access to data after signing in to the system. To manage BitLocker authentication, you can use the *BitLocker Protection Management* task. You can use this task to specify the number of computer restarts that do not require BitLocker authentication. In this way, after updates are installed and the *BitLocker Protection Management* task is complete, BitLocker authentication is automatically enabled. You can enable BitLocker authentication at any time.

How to pause BitLocker protection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Tasks**.

   The list of tasks opens.

2. Click **New task**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Industrial CyberSecurity for Nodes (5.0) → BitLocker Protection Management**.

Step 2. BitLocker Protection Management

Configure BitLocker authentication. To pause BitLocker protection, select **Temporarily allow skipping BitLocker authentication** and enter the number of restarts without BitLocker authentication (1 to 15 times). If necessary, enter an expiration date and time for the task. At the specified time, the task is automatically turned off, and the user must complete BitLocker authentication when the computer is restarted.

Step 3. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 4. Defining the task name

Enter the name of the task, for example *Updating to Windows 10*.

Step 5. Completing task creation

Finish the wizard. If necessary, select the **Run the task after the wizard finishes** check box. You can monitor the progress of the task in the task properties.

How to pause BitLocker protection using Web Console

1. In the main window of the Web Console, select **Asset management → Tasks**.

   The list of tasks opens.

2. Click **Add**.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.
2. In the **Task type** drop-down list, select **BitLocker Protection Management**.
3. In the **Task name** field, enter a brief description, for example, *Updating to Windows 10*.
4. In the **Devices to which the task will be assigned** block, select the task scope.

Step 2. BitLocker Protection Management

Configure BitLocker authentication. To pause BitLocker protection, select **Temporarily allow skipping BitLocker authentication** and enter the number of restarts without BitLocker authentication (1 to 15 times). If necessary, enter an expiration date and time for the task. At the specified time, the task is automatically turned off, and the user must complete BitLocker authentication when the computer is restarted.

Step 3. Completing task creation

Finish the wizard. A new task will be displayed in the list of tasks.

To run a task, select the check box opposite the task and click the **Start** button.

As a result, when the task is running, after the next restart of the computer, BitLocker does not prompt the user for authentication. After each restart of the computer without BitLocker authentication, Kaspersky Industrial CyberSecurity for Nodes generates a corresponding event and records the number of remaining restarts.

When the specified number of restarts or the expiration time of the task is reached, BitLocker authentication is automatically turned on. To gain access to data, the user must complete BitLocker authentication.

On computers running Windows 7, BitLocker cannot count computer restarts. Counting restarts on Windows 7 computers is handled by Kaspersky Industrial CyberSecurity for Nodes. Thus to automatically turn on BitLocker authentication after each restart, Kaspersky Industrial CyberSecurity for Nodes must be started.

To turn on BitLocker authentication ahead of time, open the *BitLocker Protection Management* task properties and select **Request authentication each time in preboot**.

Integrating with third-party systems

This section describes integration of Kaspersky Industrial CyberSecurity for Nodes with third-party features and technologies.

Performance counters for System Monitor

Performance Counters is a component of Kaspersky Industrial CyberSecurity for Nodes that you can use to monitor application performance during the operation of protection components. Kaspersky Industrial CyberSecurity for Nodes registers performance counters during installation.

It is possible to review the application performance counters using the "System Monitor" application, available in the Windows Control Panel. For detailed information on using performance counters, refer to the Microsoft Technical Support website.

Using performance counters, you can, for example, identify resource shortages when Kaspersky Industrial CyberSecurity for Nodes is running alongside other applications, as well as diagnose crashes and identify undesirable settings of Kaspersky Industrial CyberSecurity for Nodes.

Number of requests not processed due to a lack of resources

Number of requests not processed due to a lack of resources

Description	Total number of requests from the file interception driver which were not processed because of a lack of system resources (for example, RAM); counted from the time Kaspersky Industrial CyberSecurity for Nodes was last started. Kaspersky Industrial CyberSecurity for Nodes skips object processing requests that are not processed by the file interception driver.
Purpose	This counter can be used to detect and eliminate potentially lower quality in Real-Time Computer Protection that occurs because of low system resources.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, the Kaspersky Industrial CyberSecurity for Nodes process needs more RAM to process requests. Active processes of other applications may be using all available RAM.

Number of requests submitted for processing

Number of requests submitted for processing

Description	The number of objects waiting to be processed by work processes.
Purpose	This counter can be used to monitor the load on Kaspersky Industrial CyberSecurity for Nodes work processes and the overall level of file activity on the protected device.
Normal / threshold value	The counter may vary depending on the level of file activity on the protected device.

Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	N/A

Number of objects processed per second

Number of objects processed per second

Description	Number of objects processed divided by the amount of time that it took to process those objects (calculated over equal time intervals).
Purpose	This counter reflects the speed of object processing; it can be used to detect and eliminate low points in protected device performance that occur because of insufficient processor time being allotted to the Kaspersky Industrial CyberSecurity for Nodes process or errors in Kaspersky Industrial CyberSecurity for Nodes operation.
Normal / threshold value	Varies / No.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	The values of this counter depend on the values set in Kaspersky Industrial CyberSecurity for Nodes settings and the load on the protected device from other applications' processes. Observe the average counter value over an extended period of time. If the average counter value decreases, one of the following situations is possible: • The Kaspersky Industrial CyberSecurity for Nodes process does not have enough processor time to process the objects. Make sure Kaspersky Industrial CyberSecurity for Nodes receives additional processor time (by reducing other applications' load on the protected device, for example). • Kaspersky Industrial CyberSecurity for Nodes has experienced an error (several streams are idle). Restart Kaspersky Industrial CyberSecurity for Nodes.

Number of elements in the infected objects queue

Number of elements in the infected objects queue

Description	Number of infected objects currently waiting to be processed (disinfected or deleted).
Purpose	This counter can help you detect: • Interruption of Real-Time Computer Protection due to potential failures of file interception dispatchers. • Overloading of processes due to uneven distribution of processor time among different work processes and Kaspersky Industrial CyberSecurity for Nodes. • Virus outbreaks.
Normal / threshold value	This value may be something other than zero while Kaspersky Industrial CyberSecurity for Nodes is processing infected or probably infected objects but will return to zero after processing is finished / The value remains non-zero for an extended period of time.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	If the value of the counter does not return to zero for an extended period of time: • Kaspersky Industrial CyberSecurity for Nodes is not processing objects (the file interception dispatcher may have crashed). Restart Kaspersky Industrial CyberSecurity for Nodes. • There may be insufficient processor time to process the objects. Make sure Kaspersky Industrial CyberSecurity for Nodes receives additional processor time (by reducing other applications' load on the protected device, for example). • There has been a virus outbreak. A large number of infected or probably infected objects in the Real-Time File Protection component is also a sign of a virus outbreak. You can view information about the number of detected objects in the component statistics or component logs.

Total number of requests denied

Total number of requests denied

Description	**Total number of object processing requests made by the file interception driver and not accepted by the application processes; counted from the time Kaspersky Industrial CyberSecurity for Nodes was last started.** **The application skips objects for which processing requests are denied by Kaspersky Industrial CyberSecurity for Nodes processes.**
Purpose	This counter can help you detect: • Reduced Real-Time Computer Protection because Kaspersky Industrial CyberSecurity for Nodes processes are overworked. • Interruption of Real-Time Computer Protection because of failures of file interception dispatchers.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	The number of denied processing requests corresponds to the number of skipped objects. The following situations are possible depending on counter behavior: • The counter shows a few requests denied for a long time: the Kaspersky Industrial CyberSecurity for Nodes process was working at full capacity. The application was unable to scan the objects. To prevent objects being skipped, increase system resources allocated to the application. • The number of request denied significantly exceeds the critical threshold and is growing quickly: the file interception dispatcher has crashed. Kaspersky Industrial CyberSecurity for Nodes is not scanning objects when they are accessed. Restart Kaspersky Industrial CyberSecurity for Nodes.

Total number of requests skipped

Total number of requests skipped

Description	The total number of object processing requests made by the file interception driver that have been received by Kaspersky Industrial CyberSecurity for Nodes and have not generated events indicating that processing is complete; this number is counted starting from the moment when the application was last started. If an object processing request is accepted by one of the work processes but does not send an event indicating that processing is complete, the driver will transfer the request to another process and the value of the **Total Number of Skipped Requests** counter will increase by 1. If the driver has gone through all of the work processes and none of them has accepted the processing request (all were busy) or has not sent an event indicating that processing is complete, Kaspersky Industrial CyberSecurity for Nodes will skip the object, so the value of the **Total Number of Skipped Requests** counter will increase by 1.
Purpose	This counter enables you to detect drops in performance due to failures of file interception dispatchers.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter is anything other than zero, this means that one or more file interception dispatcher streams have frozen and are down. The counter value corresponds to the number of streams currently down. If the scan speed is not satisfactory, restart Kaspersky Industrial CyberSecurity for Nodes to restore the off-line streams.

Maximum number of file interception dispatcher streams

Starting from Kaspersky Industrial CyberSecurity for Nodes version 5.0, the "Maximum number of file interception dispatcher streams" counter is not supported.

Average number of file interception dispatcher streams

Starting from Kaspersky Industrial CyberSecurity for Nodes version 5.0, the "Average number of file interception dispatcher streams" counter is not supported.

Kaspersky Industrial CyberSecurity for Nodes SNMP counters and traps

If you included the SNMP Protocol Support component in the set of anti-virus components to be installed, you can view Kaspersky Industrial CyberSecurity for Nodes counters and traps using Simple Network Management Protocol (SNMP).

To view Kaspersky Industrial CyberSecurity for Nodes counters and traps from the administrator's workstation, start SNMP Service on the protected device and start SNMP and SNMP Trap Services on the administrator's workstation.

Kaspersky Industrial CyberSecurity for Nodes SNMP counters

This section contains tables with a description of the settings for Kaspersky Industrial CyberSecurity for Nodes SNMP counters.

Performance counters

Performance counters

Counter	Definition
currentRequestsAmount	Number of requests submitted for processing
currentInfectedQueueLength	Number of elements in the infected objects queue
currentObjectProcessingRate	Number of objects processed per second
currentWorkProcessesNumber	Current number of work processes used by Kaspersky Industrial CyberSecurity for Nodes

Backup counter

Backup counter

Counter	Definition
currentBackupStorageSize	Total amount of data in Backup (MB)

General counters

General counters

Counter	Definition
lastCriticalAreasScanAge	The time interval in seconds since the task *Critical Areas Scan* was completed.
licenseExpirationDate	License expiration date. If an active and additional key have been added, the date of expiry of the license associated with the additional key is displayed.
currentApplicationUptime	The amount of time that Kaspersky Industrial CyberSecurity for Nodes has been running since it was last started, in hundredths of seconds.

Update counter

Update counter

Counter	Definition
avBasesAge	Time elapsed in hundredths of seconds since the creation date of the latest installed database updates.

Real-Time File Protection counters

Real-Time File Protection counters

Counter	Definition
totalObjectsProcessed	Total number of objects scanned since the last launch of the Real-Time File Protection component
totalInfectedObjectsFound	Total number of infected and other objects detected since the last launch of the Real-Time File Protection component
totalSuspiciousObjectsFound	Total number of probably infected objects detected since the last launch of the Real-Time File Protection component
totalVirusesFound	Total number of objects detected since the last launch of the Real-Time File Protection component
totalObjectsQuarantined	Total number of infected, probably infected and other objects which were placed into Quarantine by Kaspersky Industrial CyberSecurity for Nodes; calculated from the time the Real-Time File Protection component was last launched
totalObjectsNotQuarantined	Total number of infected or probably infected objects Kaspersky Industrial CyberSecurity for Nodes attempted to quarantine but was unable to; calculated from the time the Real-Time File Protection component was last launched
totalObjectsDisinfected	Total number of infected objects disinfected by Kaspersky Industrial CyberSecurity for Nodes; calculated from the time the Real-Time File Protection component was last launched
totalObjectsNotDisinfected	Total number of infected and other objects which Kaspersky Industrial CyberSecurity for Nodes attempted to disinfect but was unable to; calculated from the time the Real-Time File Protection component was last launched
totalObjectsDeleted	Total number of infected, probably infected and other objects which were deleted by Kaspersky Industrial CyberSecurity for Nodes; calculated from the time the Real-Time File Protection component was last launched
totalObjectsNotDeleted	Total number of infected, probably infected and other objects which Kaspersky Industrial CyberSecurity for Nodes attempted to delete but was unable to; calculated from the time the Real-Time File Protection component was last launched
totalObjectsBackedUp	Total number of infected objects and other which were placed into Backup by Kaspersky Industrial CyberSecurity for Nodes; calculated from the time the Real-Time File Protection component was last launched
totalObjectsNotBackedUp	Total number of infected objects and other which Kaspersky Industrial CyberSecurity for Nodes attempted to place into Backup but was unable to; calculated from the time the Real-Time File Protection component was last launched

Counter	Definition
currentFileMonitorTaskStatus	Status of the Real-Time File Protection component: • `1` means the component is enabled and is providing protection. • `0` means the component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.

AMSI Scanner counters

AMSI Scanner counters

Counter	Definition
currentScriptCheckerTaskStatus	Status of the AMSI Scanner component: • `1` means the component is enabled and is providing protection. • `0` means the component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
totalScriptsProcessed	Number of scripts processed since the last launch of the AMSI Scanner component.
totalInfectedIDangerousScriptsFound	Number of dangerous scripts detected since the last launch of the AMSI Scanner component.
totalSuspiciousScriptsFound	Total number of suspicious scripts detected since the last launch of the AMSI Scanner component.
totalScriptsBlocked	Total number of scripts blocked since the last launch of the AMSI Scanner component. The counter value changes if the component is enabled in the **Block**, and is equal to the value of the totalInfectedIDangerousScriptsFound counter.

Kaspersky Industrial CyberSecurity for Nodes SNMP traps and their options

The SNMP traps options in Kaspersky Industrial CyberSecurity for Nodes are summarized as follows:

- eventThreatDetected: Object detected.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: Maximum Backup size exceeded. The total amount of data in Backup exceeds the value specified by **Limit the size of Backup to**. Kaspersky Industrial CyberSecurity for Nodes continues to back up infected objects.

The trap has the following options:

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdBackupStorageSizeExceeds: Backup free space threshold exceeded. The amount of free space in Backup is less than or equal to the value specified by **Threshold value for available space (MB)**. Kaspersky Industrial CyberSecurity for Nodes continues to back up infected objects.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotBackuped: Object not backed up.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventBackupInternalError: Backup error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Databases are out of date. Number of days since the last time the *Update* task (local task, group task, or task for sets of protected devices) was run.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime

- eventSource
- days

- eventAVBasesTotallyOutdated: Databases are extremely out of date. Number of days since the last time the *Update* task (local task, group task, or task for sets of protected devices) was run.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: Application started.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: Application stopped.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Critical areas scan has not been performed for a long time. The number of days since the *Critical Areas Scan* task was last completed.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired: License expired.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: License expires soon. Calculated as the number of days until the expiration date for the license.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Task completion error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Error while running the *Update* task.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason
  - eventSource

Kaspersky Industrial CyberSecurity for Nodes SNMP traps options descriptions and possible values

Descriptions of the traps options and their possible values are given below:

- eventDateAndTime: event date and time
- eventSeverity: importance level

The option can take the following values:

- critical (1) – critical
- warning (2) – warning
- info (3) – informational

- userName: user name (for example, the name of a user that attempted to access an infected file).
- computerName: protected device name (for example, the name of a protected device from which a user attempted to access an infected file).
- eventSource: functional component that generated the event.

  The option can take the following values:

  - unknown (0) – Functional component unknown
  - quarantine (1) – Quarantine
  - backup (2) – Backup
  - reporting (3) – Task logs
  - updates (4) – Update
  - realTimeProtection (5) – Real-Time File Protection
  - onDemandScanning (6) – On-Demand Scan
  - product (7) – event related to operation of Kaspersky Industrial CyberSecurity for Nodes as a whole rather than operation of individual components
  - systemAudit (8) – system audit log
- eventReason: event trigger: what triggered the event.

  The option can take the following values:

  - reasonUnknown (0) – reason is unknown.
  - reasonInvalidSettings (1) – only for Backup and Quarantine events. Displayed if the Quarantine or Backup folder is unavailable (insufficient access permissions or an invalid folder is specified in the Quarantine settings, for example, a network path is specified). In this case, Kaspersky Industrial CyberSecurity for Nodes will use the default Backup or Quarantine folder.
- objectName: an object name (for example, the name of the file where the virus was detected).
- threatName: The name of the object according to the Virus Encyclopedia classification. This name is included in the full name that Kaspersky Industrial CyberSecurity for Nodes returns on detecting an object. You can view the full name of a detected object in the task log.
- detectType: type of object detected.

The option can take the following values:

- undefined (0) – Not defined
- virware – Classic viruses and network worms
- trojware – Trojans
- malware – Other malicious applications
- adware – Advertising software
- pornware – Pornographic software
- riskware – Legitimate applications that may be used by intruders to damage the user's device or personal data

- detectCertainty: certainty level for threat detection.

  The option can take the following values:

  - Suspicion (probably infected) – Kaspersky Industrial CyberSecurity for Nodes has detected a partial match between a section of object code and a known section of malicious code.
  - Sure (infected) – Kaspersky Industrial CyberSecurity for Nodes has detected a complete match between a section of code in the object and a known section of malicious code.

- days: number of days (for example, the number of days until the license expiration date).
- errorCode: an error code.
- taskName: task name.
- updaterErrorEventReason: the reason for the update error.

  The option can take the following values:

  - reasonUnknown(0) – reason is unknown.
  - reasonAccessDenied – access denied.
  - reasonUrlsExhausted – the list of update sources has been exhausted.
  - reasonInvalidConfig – invalid configuration file.
  - reasonInvalidSignature – invalid signature.
  - reasonCantCreateFolder – folder cannot be created.
  - reasonFileOperError – file error.
  - reasonDataCorrupted – object corrupted.
  - reasonConnectionReset – connection reset.
  - reasonTimeOut – connection timeout exceeded.

- reasonProxyAuthError – proxy authentication error.
- reasonServerAuthError – server authentication error.
- reasonHostNotFound – device not found.
- reasonServerBusy – server unavailable.
- reasonConnectionError – connection error.
- reasonModuleNotFound – object not found.
- reasonBlstCheckFailed (16) – error while checking the key denylist. It is possible that database updates were being published at the time of the update; please repeat the update in a few minutes.

- storageObjectNotAthreatddedEventReason: the reason why the object was not put in Backup or Quarantine.

  The option can take the following values:

  - reasonUnknown (0) – reason is unknown.
  - reasonStorageInternalError – database error; Kaspersky Industrial CyberSecurity for Nodes must be restored.
  - reasonStorageReadOnly – database is read-only; Kaspersky Industrial CyberSecurity for Nodes must be restored.
  - reasonStorageIOError – input-output error: a) Kaspersky Industrial CyberSecurity for Nodes is corrupted and needs to be restored; b) the disk where Kaspersky Industrial CyberSecurity for Nodes files are stored is corrupted.
  - reasonStorageCorrupted – storage is corrupted; Kaspersky Industrial CyberSecurity for Nodes must be restored.
  - reasonStorageFull – database is full; free disk space is required.
  - reasonStorageOpenError – database file could not be opened; Kaspersky Industrial CyberSecurity for Nodes must be restored.
  - reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Industrial CyberSecurity for Nodes requirements.
  - reasonObjectNotFound – object being placed in Quarantine does not exist on the disk.
  - reasonObjectAccessError – insufficient permissions to use Backup API: the account being used to perform the operation does not have Backup Operator permissions.
  - reasonDiskOutOfSpace – not enough space on the disk.

WMI Integration

Kaspersky Industrial CyberSecurity for Nodes supports integration with Windows Management Instrumentation (WMI): you can use client systems that use WMI to receive data via the Web-Based Enterprise Management (WBEM) standard in order to receive information about the status of Kaspersky Industrial CyberSecurity for Nodes and its components.

When Kaspersky Industrial CyberSecurity for Nodes is installed, it registers a proprietary module on the system to create a Kaspersky Industrial CyberSecurity for Nodes namespace on the protected device. A Kaspersky Industrial CyberSecurity for Nodes namespace lets you work with Kaspersky Industrial CyberSecurity for Nodes classes and instances and their properties.

The values of some instance properties depend on task types.

A *non-periodic task* is an application task that is not time-limited and can either be constantly running or stopped. Such tasks have no execution progress. The task results are logged continuously while the task is running as single events (for example, detection of an infected object by any Real-Time Computer Protection tasks). This type of tasks is managed via Kaspersky Security Center policies.

A *periodic task* is an application task that is time-limited and has execution progress displayed as a percentage. The task results are generated when the task is complete and are represented as a single item or changed application state (for example, completed application database update, generated configuration files for rule generation tasks). Several periodic tasks of the same type can run on a single protected device simultaneously (e.g. three On-Demand scan tasks with different scan scopes). Periodic tasks can be managed via Kaspersky Security Center as group tasks.

If you use tools to generate WMI namespace queries and receive dynamic data from WMI namespaces on your corporate network, you will be able to receive information about the current application state (see the table below).

Information about the application state

Instance property	Description	Values
`ProductName`	Name of the installed application.	Full name of the application without version number.
`ProductVersion`	Full version number of the installed application.	Full application version number, including the build number.
`InstalledPatches`	Set of display names for installed patches.	List of critical fixes installed for the application.
`IsLicenseInstalled`	Application activation status.	Status of the key used to activate the application. Possible values: • `False` No license key has been added. • `True` A license key has been added.
`LicenseDaysLeft`	Shows how many days are left before a current license expiration.	Number of days remaining before expiration of the current license. Possible non-positive values: • `0` License has expired. • `-1` Unable to get information on the current key or the specified key cannot be used to activate the application (for example, it is blocked based on key denylist).
`AVBasesDatetime`	Timestamp for the current anti-virus database version.	Date and time of the creation of the anti-virus databases currently in use. If the installed application does not use anti-virus databases, then the field has the `{Not installed}` value.

Instance property	Description	Values
`IsExploitPreventionEnabled`	Status of the Exploit Prevention component.	Status of the Exploit Prevention component. Possible values: • `True` The Exploit Prevention component is enabled and is providing protection. • `False` The Exploit Prevention component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
`ProtectionTasksRunning`	Set of protection tasks that are currently running.	List of protection, control, and monitoring tasks currently running. This field should account for all running non-periodic tasks. If no non-periodic task is running, the field has the `{No}` value.
`IsAppControlRunning`	Status of the Applications Launch Control component.	Possible values • `True` The Applications Launch Control component is enabled and is providing protection. • `False` The Applications Launch Control component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
`AppControlMode`	The Applications Launch Control component operating mode.	Possible values: • `Active` The **Block** mode is specified in component settings. • `Statistics Only` The **Inform** mode is specified in component settings. • `Not installed` The Applications Launch Control component is not installed. • `Unknown` The component is disabled.
`AppControlRulesNumber`	Total number of applications launch control rules.	The number of rules specified in the settings of the Applications Launch Control component at the current moment.
`AppControlLastBlocking`	The timestamp for the last application launch blocking by the Applications Launch Control component in any mode.	Date and time for the last application launch blocking by the Applications Launch Control component. This field includes all blocked applications, regardless of the operating mode of the component. If no instances of blocked application launches are registered at the time the WMI query is processed, the field is assigned the `{No}` value.
`PeriodicTasksRunning`	Set of periodic tasks that are currently running.	List of On-Demand Scan, Update, and inventory-taking tasks currently running. This field should include all running periodic tasks. If no periodic tasks are currently running, then the field has the `{No}` value.
`ConnectionState`	Status of the connection between the WMI Provider component and the Kaspersky Industrial CyberSecurity for Nodes Service.	Information about the status of the connection between the WMI Provider component and the Kaspersky Industrial CyberSecurity for Nodes Service. Possible values: • `Success` Connection was successfully established: the WMI client can receive the application status. • `Failed. Error Code: <code>` Connection could not be established due to an error with the specified code.
`IsDumpingEnabled`	Memory dump recording status.	Possible values • `True` Memory dump recording is enabled. • `False` Memory dump recording is disabled.
`DumpsFolder`	Folder for storing dump files.	Full folder path. If dump recording is disabled, this field is empty.
`IsTracingEnabled`	Application tracing status.	Possible values • `True` Application tracing is enabled. • `False` Application tracing is disabled.
`TraceFolder`	Folder for storing trace files.	Full folder path. If application tracing is disabled, this field is empty.

Instance property	Description	Values
`AllTasksState`	The status of all tasks.	Information about the status of tasks in the `{<profile-name_1>, <profile-type_1>, <profile-state_1>,...<profile-name_N>, <profile-type_N>, <profile-state_N>}` format, where `profile-name` is the name of the task, `profile-type` is the type of the task, and `profile-state` is the current status of the task. Possible status values: • `not started` The task has not been started yet. • `running` The task is running. • `running ma` The task is running; a fault occurred while running. • `paused` The task is paused. • `stopped` The task is stopped. • `completed` The task has completed successfully. • `failed` The task ended with an error. • `disabled` The task is disabled and cannot be run. • `starting` The task is in the process of starting. • `pausing` The task is in the process of being paused. • `stopping` The task is in the process of being stopped. • `<unknown>` Cannot determine the status.
`IsDevControlRunning`	Status of the Device Control component.	Possible values: • `True` The Device Control component is enabled and is providing protection. • `False` The Device Control component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
`IsKSNRunning`	Status of the Kaspersky Security Network component.	Possible values: • `True` The Kaspersky Security Network component is enabled and is providing protection. • `False` The Kaspersky Security Network component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
`IsOASRunning`	Status of the Real-Time File Protection component.	Possible values: • `True` The Real-Time File Protection component is enabled and is providing protection. • `False` The Real-Time File Protection component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.

This data represents instance properties `KasperskySecurity_ProductInfo.ProductName=Kaspersky Industrial CyberSecurity for Nodes`, where:

- `KasperskySecurity_ProductInfo` is the name of the Kaspersky Industrial CyberSecurity for Nodes class.
- `.ProductName=Kaspersky Industrial CyberSecurity for Nodes` are key properties of Kaspersky Industrial CyberSecurity for Nodes.

The class is instantiated in the `ROOT\Kaspersky\Security` namespace.

Kaspersky Industrial CyberSecurity for Nodes database and software modules update

This section contains information about update tasks and rollback of Kaspersky Industrial CyberSecurity for Nodes updates, as well as task configuration instructions.

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

Updating databases and application modules

Updating the databases and application modules of Kaspersky Industrial CyberSecurity for Nodes ensures up-to-date protection on your computer. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Industrial CyberSecurity for Nodes databases contain information about threats and ways of neutralizing them. To detect threats quickly, you are urged to regularly update the databases and application modules.

Regular updates require a license in effect. If there is no current license, you will be able to perform an update only once.

Kaspersky Industrial CyberSecurity for Nodes downloads updates of application databases and modules from Kaspersky's HTTP or FTP update servers, Kaspersky Security Center Administration Server, or other update sources.

You can download updates to each protected device or use one protected device as an intermediary. Updates will be copied to it, and then distributed to protected devices. If you manage your organization's device security centrally with Kaspersky Security Center, you can leverage the Administration Server to act as a proxy for downloading updates.

If the update download process is interrupted or results in an error Kaspersky Industrial CyberSecurity for Nodes will automatically switch back to using the databases from the last installed updates. If the Kaspersky Industrial CyberSecurity for Nodes databases become corrupted, they can be manually rolled back to previously installed updates.

While performing an update, the following objects are downloaded and installed on your computer:

- Kaspersky Industrial CyberSecurity for Nodes databases. Computer protection is provided using databases that contain signatures of viruses and other threats and information on ways to neutralize them. Protection components use this information when searching for and neutralizing infected files on your computer. The databases are constantly updated with records of new threats and methods for counteracting them. Therefore, we recommend that you update the databases regularly.

  In addition to the Kaspersky Industrial CyberSecurity for Nodes databases, the network drivers that enable the application's components to intercept network traffic are updated.

- Application modules. Updating the application modules fixes vulnerabilities in Kaspersky Industrial CyberSecurity for Nodes, adds new functions, or enhances existing functions.

While updating, the application modules and databases on your computer are compared against the up-to-date version at the update source. If your current databases and application modules differ from their respective up-to-date versions, the missing portion of the updates is installed on your computer.

If the databases are obsolete, the update package may be large, which may cause additional internet traffic (up to several dozen MB).

Information about the current state of the Kaspersky Industrial CyberSecurity for Nodes databases is displayed in the main application window or the tooltip that you see when you hover the cursor over the icon of the application in the notification area.

Information on update results and on all events that occur during the performance of the update task is logged in the update task log.

About Update tasks

Kaspersky Industrial CyberSecurity for Nodes has two update tasks: *Update* and *Update rollback*.

Update

By default, Kaspersky Industrial CyberSecurity for Nodes copies databases and, if available, application modules from the update source to the device and immediately starts using them in protection components. The On-Demand Scan tasks start using the updated database at the next start.

You can configure the settings of the *Update* task. When task settings are modified, Kaspersky Industrial CyberSecurity for Nodes will apply the new values at the next task start.

By default, the *Update* task is set to **Manually** mode. You are not allowed to pause and resume Update tasks.

Update rollback

The task makes Kaspersky Industrial CyberSecurity for Nodes go back to the previous databases and application modules.

The *Update rollback* task is disabled by default.

Kaspersky Industrial CyberSecurity for Nodes databases and modules update schemes

The choice of update source in the *Update* task depends on the update scheme for databases and software modules used in the organization.

Kaspersky Industrial CyberSecurity for Nodes databases and modules can be updated on the protected devices using the following schemes:

- Download updates directly from the Internet to each protected device (Scheme 1).
- Download updates from the Internet to an intermediate device and distribute updates to protected devices from that device.

  Any device on which the following applications are installed can serve as an intermediary:

  - Kaspersky Industrial CyberSecurity for Nodes (Scheme 2).
  - Kaspersky Security Center Administration Server (Scheme 3).

  > Updating using an intermediate device not only reduces Internet traffic, but also provides additional network protected device security.

- Download database updates to each protected device via a secure removable drive (scheme 4).

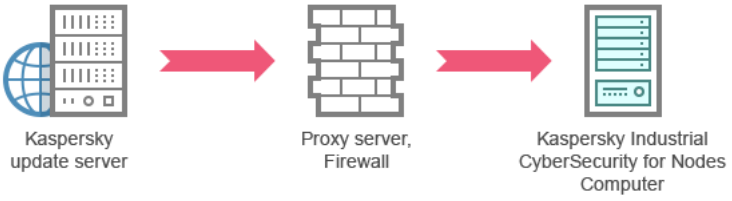
The update schemes listed are described below.

Scheme 1. Updating databases and modules directly from the Internet

To configure Kaspersky Industrial CyberSecurity for Nodes updates directly from the Internet:

on each protected device in the settings of the *Update* task specify Kaspersky's update servers as the source of updates.

Other HTTPS or HTTP servers that have an update folder can be configured as the update source.



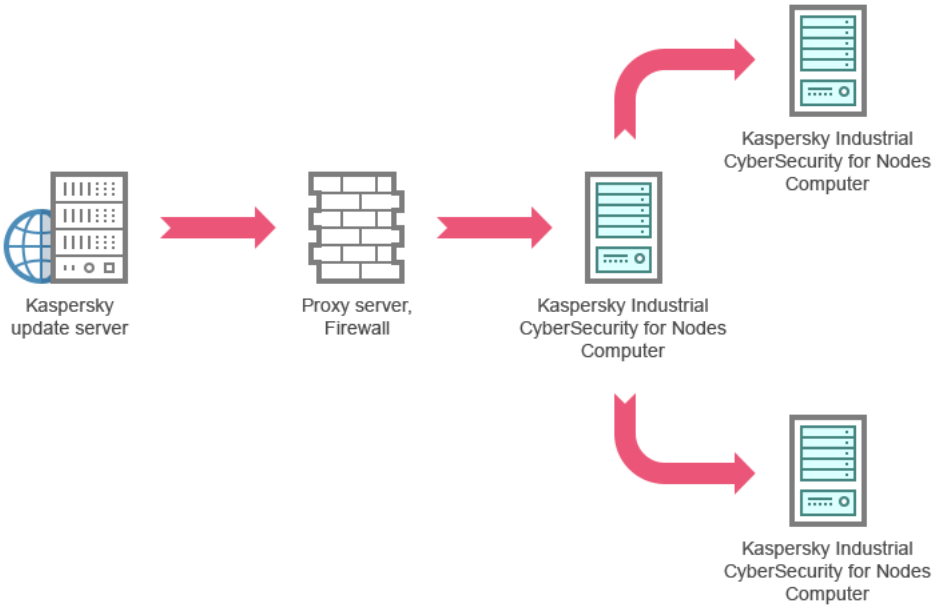
Scheme 1: Updating databases and modules directly from the Internet

Scheme 2. Updating databases and modules via one of the protected devices

To configure receiving updates for Kaspersky Industrial CyberSecurity for Nodes via one of the protected devices:

1. Copy updates to the selected protected device.
   - Configure the *Update* task settings on the selected protected device:
     a. Specify Kaspersky's update server as the update source.
     b. Specify a shared folder to be used as the folder where updates are saved.
2. Distribute updates to other protected devices:
   - Configure the *Update* task on each of the protected devices:
     a. For the update source, specify a folder on the intermediate device's drive to which updates will be downloaded.

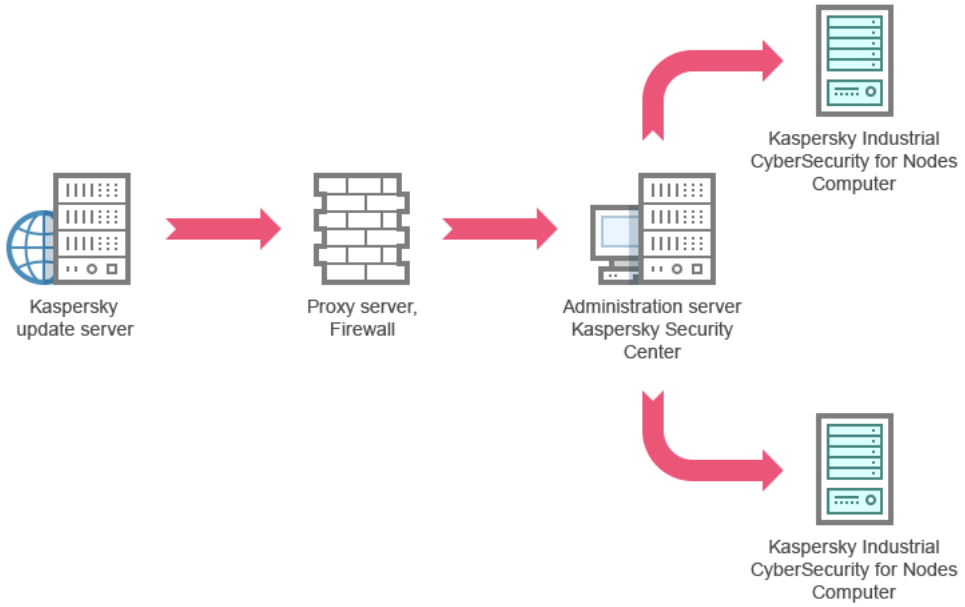
Kaspersky Industrial CyberSecurity for Nodes will obtain updates via one of the protected devices.



Scheme 2: Updating databases and modules via one of the protected devices

Scheme 3. Updating databases and modules via Kaspersky Security Center Administration Server

If you are using Kaspersky Security Center to centrally manage antivirus protection for devices, you can download updates via the Kaspersky Security Center Administration Server installed on your local network.



Scheme 3: Updating databases and modules via Kaspersky Security Center Administration Server

In order to configure receiving updates for Kaspersky Industrial CyberSecurity for Nodes via the Kaspersky Security Center Administration Server:

1. Install the Network Agent on each of the protected devices. The Network Agent is a software component included in the Kaspersky Security Center distribution kit. This ensures interaction between the Administration Server and Kaspersky Industrial CyberSecurity for Nodes on the protected device. Detailed information about Network Agent and its configuration using Kaspersky Security Center is provided in the Kaspersky Security Center Help.

2. Download updates from Kaspersky update servers to Kaspersky Security Center Administration Server.

   - Configure the *Download updates to the Administration Server repository* task for the specified set of protected devices:

     a. Specify Kaspersky's update server as the update source.

3. Distribute updates to protected devices. To do so, perform one of the following actions:

   - On the Kaspersky Security Center Administration Server configure the *Update* group task to distribute updates to protected devices:

   - Configure the *Update* task on each of the protected devices:

     a. Specify the Kaspersky Security Center Administration Server as the update source.

     b. Configure the task schedule if necessary.

Kaspersky Industrial CyberSecurity for Nodes will obtain updates via the Kaspersky Security Center Administration Server.

Scheme 4. Updating application databases from a secure removable drive

To update the Kaspersky Industrial CyberSecurity for Nodes databases using a secure removable drive:

1. Connect the secure removable drive to the device on which Kaspersky Industrial CyberSecurity for Nodes is installed and which has access to the application database updates.
2. Add an allowing rule of the Device Control component for the connected removable drive.
3. In the Application Console, configure and run the *Secure copying of application databases* task.
4. Connect the secure removable drive containing the database updates to the device on which you need to update the application databases.
5. In the Application Console, configure and run the *Secure update of application databases* task.

Kaspersky Industrial CyberSecurity for Nodes will receive the updated application databases from the secure removable drive.

Configuring Update tasks

How to configure the Update task in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console, go to the local or group update task that you want to configure.
2. Open the **Settings** section.
3. Under **Update settings for local mode** for Kaspersky Industrial CyberSecurity for Nodes connected to the Kaspersky Security Center Administration Server, configure update sources:

   a. Click **Settings**.

   The **Update of databases and application modules** window opens.

   b. Select the check box next to update sources that you want to use:

   - Kaspersky Security Center Administration Server
   - Kaspersky update servers

   If necessary, click the **Add** button to add a custom update source.

   c. If you select multiple update sources, use the **Up** and **Down** buttons to order the update sources by priority. Kaspersky Industrial CyberSecurity for Nodes accesses the update sources strictly following the configured order and performs the update task using the update package from the first available update source.

   By default, Kaspersky Industrial CyberSecurity for Nodes uses the Kaspersky Security Center server as the first update source. This helps conserve traffic when updating. If a policy is not applied to the computer, Kaspersky servers are selected as the first update source in the settings of the local *Update* task because the application may not have access to Kaspersky Security Center.

d. If you selected **Kaspersky update servers** as the update source, select the principle that Kaspersky Industrial CyberSecurity for Nodes must follow when selecting a Kaspersky update server:

- **Detect automatically**. The application uses the nearest available Kaspersky update server.
- **Select from the list**. The application uses the Kaspersky update server in the country selected in the list.

e. In the **Update of databases and application modules** window, click the **OK** button.

4. Configure application database updates:

a. Select or clear the **Download updates of application databases** check box.

b. Select or clear the **Lower the load on the disk I/O** check box. This check box enables or disables the process whereby the disk subsystem is optimized by storing update files on a virtual drive in RAM. By default, the check box is cleared.

c. If you selected the **Lower the load on the disk I/O** check box, in the **RAM used for optimization, MB** field, specify the amount of RAM in megabytes. The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 640 MB. The minimum RAM size is 400 MB.

When running the *Update* task with the disk subsystem optimization feature enabled, one of the following may occur:

- If the value is too small, the allocated amount of RAM might be insufficient to complete the database update task (for example, during the first update), which will lead to the completion of the task with an error.

  In this case, it is recommended to allocate more RAM for the disk subsystem optimization feature.

- If the value is too large, at the start of the Database Update task, it might be impossible to create a virtual drive of a selected size in RAM. As a result, the disk subsystem optimization feature automatically disables, and the Database Update task runs without the optimization feature.

  In this case, it is recommended to allocate less RAM for the disk subsystem optimization feature.

5. Configure application software module updates:

a. Select or clear the **Download updates of application modules** check box.

If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes notifies the user about available application module updates and includes application module updates in the update package while running the *Update* task. The type of application module updates that will be applied is configured separately. The check box is selected by default.

b. Select the application module update type that you want to apply.

- **Install critical and approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs critical updates automatically and all other application module updates only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center.
- **Install only approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs them only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center. This option is selected by default.

If application module updates require reviewing and accepting the terms of the End User License Agreement, the application installs updates after the terms of the End User License Agreement have been accepted.

6. Configure the copying of updates to a folder for local storage:

   a. Select or clear the **Copy updates to a folder for local storage** check box.

   b. Select the contents of updates that you want the application to copy to the local storage folder:

   - **Copy database updates**. The application downloads only database updates.
   - **Copy critical application modules updates**. The application downloads only critical application module updates.
   - **Copy database updates and critical updates of application modules**. The application downloads database updates and critical application module updates.

   c. Specify the local or network folder to which Kaspersky Industrial CyberSecurity for Nodes will be distributing downloaded updates.

7. Save your changes.

How to configure the Update task in the Application Console

1. In the Application Console tree, open the **Update** → **Update of databases and application modules** node.
2. Click the **Properties** link in the results pane.

   The **Properties: Update of databases and application modules** window opens.
3. Under **Update settings for local mode** for Kaspersky Industrial CyberSecurity for Nodes connected to the Kaspersky Security Center Administration Server, configure update sources:

   a. Click **Settings**.

   The **Update of databases and application modules** window opens.

   b. Select the check box next to update sources that you want to use:

   - Kaspersky Security Center Administration Server
   - Kaspersky update servers

   If necessary, click the **Add** button to add a custom update source.

   c. If you select multiple update sources, use the **Up** and **Down** buttons to order the update sources by priority. Kaspersky Industrial CyberSecurity for Nodes accesses the update sources strictly following the configured order and performs the update task using the update package from the first available update source.

   By default, Kaspersky Industrial CyberSecurity for Nodes uses the Kaspersky Security Center server as the first update source. This helps conserve traffic when updating. If a policy is not applied to the computer, Kaspersky servers are selected as the first update source in the settings of the local *Update* task because the application may not have access to Kaspersky Security Center.

d. If you selected **Kaspersky update servers** as the update source, select the principle that Kaspersky Industrial CyberSecurity for Nodes must follow when selecting a Kaspersky update server:

- **Detect automatically**. The application uses the nearest available Kaspersky update server.
- **Select from the list**. The application uses the Kaspersky update server in the country selected in the list.

e. In the **Update of databases and application modules** window, click the **OK** button.

4. Configure application database updates:

a. Select or clear the **Download updates of application databases** check box.

b. Select or clear the **Lower the load on the disk I/O** check box. This check box enables or disables the process whereby the disk subsystem is optimized by storing update files on a virtual drive in RAM. By default, the check box is cleared.

c. If you selected the **Lower the load on the disk I/O** check box, in the **RAM used for optimization, MB** field, specify the amount of RAM in megabytes. The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 640 MB. The minimum RAM size is 400 MB.

When running the *Update* task with the disk subsystem optimization feature enabled, one of the following may occur:

- If the value is too small, the allocated amount of RAM might be insufficient to complete the database update task (for example, during the first update), which will lead to the completion of the task with an error.

  In this case, it is recommended to allocate more RAM for the disk subsystem optimization feature.

- If the value is too large, at the start of the Database Update task, it might be impossible to create a virtual drive of a selected size in RAM. As a result, the disk subsystem optimization feature automatically disables, and the Database Update task runs without the optimization feature.

  In this case, it is recommended to allocate less RAM for the disk subsystem optimization feature.

5. Configure application software module updates:

a. Select or clear the **Download updates of application modules** check box.

If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes notifies the user about available application module updates and includes application module updates in the update package while running the *Update* task. The type of application module updates that will be applied is configured separately. The check box is selected by default.

b. Select the application module update type that you want to apply.

- **Install critical and approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs critical updates automatically and all other application module updates only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center.
- **Install only approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs them only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center. This option is selected by default.

If application module updates require reviewing and accepting the terms of the End User License Agreement, the application installs updates after the terms of the End User License Agreement have been accepted.

6. Configure the copying of updates to a folder for local storage:

   a. Select or clear the **Copy updates to a folder for local storage** check box.

   b. Select the contents of updates that you want the application to copy to the local storage folder:

      - **Copy database updates**. The application downloads only database updates.
      - **Copy critical application modules updates**. The application downloads only critical application module updates.
      - **Copy database updates and critical updates of application modules**. The application downloads database updates and critical application module updates.

   c. Specify the local or network folder to which Kaspersky Industrial CyberSecurity for Nodes will be distributing downloaded updates.

7. Save your changes.

How to configure the Update task in the Kaspersky Security Center Web Console

1. In the Web Console, go to the local or group *Update* task that you want to configure.
2. Open the **Settings** section.
3. Select the **Local mode** tab to configure the *Update* task for Kaspersky Industrial CyberSecurity for Nodes connected to the Kaspersky Security Center Administration Server.
4. Configure update sources:

   a. Under **Update sources**, select the check box next to update sources that you want to use:

      - **Kaspersky Security Center Administration Server**
      - **Kaspersky update servers**

      If necessary, click the **Add** button to add a custom update source.

   b. If you select multiple update sources, use the **Up** and **Down** buttons to order the update sources by priority. Kaspersky Industrial CyberSecurity for Nodes accesses the update sources strictly following the configured order and performs the update task using the update package from the first available update source.

      By default, Kaspersky Industrial CyberSecurity for Nodes uses the Kaspersky Security Center server as the first update source. This helps conserve traffic when updating. If a policy is not applied to the computer, Kaspersky servers are selected as the first update source in the settings of the local *Update* task because the application may not have access to Kaspersky Security Center.

5. Configure application database updates:

   a. Select or clear the **Download updates of application databases** check box.

   b. Select or clear the **Lower the load on the disk I/O** check box. This check box enables or disables the process whereby the disk subsystem is optimized by storing update files on a virtual drive in RAM. By default, the check box is cleared.

   c. If you selected the **Lower the load on the disk I/O** check box, in the **RAM used for optimization, MB** field, specify the amount of RAM in megabytes. The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 640 MB. The minimum RAM size is 400 MB.

   When running the *Update* task with the disk subsystem optimization feature enabled, one of the following may occur:

   - If the value is too small, the allocated amount of RAM might be insufficient to complete the task (for example, during the first update), which will lead to the completion of the task with an error.

     In this case, it is recommended to allocate more RAM for the disk subsystem optimization feature.

   - If the value is too large, at the start of the task, it might be impossible to create a virtual drive of a selected size in RAM. As a result, the disk subsystem optimization feature automatically disables, and the Database Update task runs without the optimization feature.

     In this case, it is recommended to allocate less RAM for the disk subsystem optimization feature.

6. Configure application software module updates:

   a. Select or clear the **Download updates of application modules** check box.

   If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes notifies the user about available application module updates and includes application module updates in the update package while running the *Update* task. The type of application module updates that will be applied is configured separately. The check box is selected by default.

   b. Select the application module update type that you want to apply.

   - **Install critical and approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs critical updates automatically and all other application module updates only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center.

   - **Install only approved updates**. If this option is selected, when application module updates are available Kaspersky Industrial CyberSecurity for Nodes installs them only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center. This option is selected by default.

   If application module updates require reviewing and accepting the terms of the End User License Agreement, the application installs updates after the terms of the End User License Agreement have been accepted.

7. Configure the copying of updates to a folder for local storage:

   a. Select or clear the **Copy updates to folder** check box.

   b. Select the contents of updates that you want the application to copy to the local storage folder:

   - **Copy database updates**. The application downloads only database updates.
   - **Copy critical application modules updates**. The application downloads only critical application module updates.
   - **Copy database updates and critical updates of application modules**. The application downloads database updates and critical application module updates.

   c. Specify the local or network folder to which Kaspersky Industrial CyberSecurity for Nodes will be distributing downloaded updates.

8. Save your changes.

SMU update of the application

To update the application using the Kaspersky update service (Seamless Update; SMU), you do not need to run the installer, in contrast to other update methods. Kaspersky Industrial CyberSecurity for Nodes gets the new version of the application alongside anti-virus databases from the same source.

An SMU update allows updating the application on all computers of your organization to the latest version. Before applying an SMU update, we recommend testing the new version of the application on a few computers. To do so, you must update the application on these computers manually (for example, locally using the Setup Wizard). You cannot select individual computers when performing an SMU update.

The update schedule for the application is determined by Kaspersky staff. To make sure the new version of the application is running smoothly, Kaspersky makes updates available on a step by step basis. This means you may get your SMU update up to two months later than a new version is released.

You can manage the SMU update of the application using the *Update* task. To have the new version of the application included in the same package as the anti-virus databases, you must allow updating *application modules* in *Update* task settings.

Steps of an SMU update of the application

1. **After a new version of the application is released or a module is updated, Kaspersky distributes an update.**
2. **The user approves the update of the application.**

   If the computer is connected to the Kaspersky Security Center, the update is available in the Kaspersky Security Center, in the **Updates for Kaspersky databases and software modules** section. For more details on approving updates, refer to the Kaspersky Security Center Help.

   If the computer is not connected to Kaspersky Security Center, the update is available in the Application Console. To approve the update, go to the **Update** → **Application update** section, select an application version and, if necessary, accept the terms and conditions of agreements.
3. **Kaspersky Industrial CyberSecurity for Nodes runs the Update task on a schedule.**

As a result, Kaspersky Industrial CyberSecurity for Nodes updates the application in "silent" mode.

Secure copying of application databases

The task can only be configured in the Application Console. This task cannot be configured in the Kaspersky Security Center Management Console or Kaspersky Security Center Web Console.

To configure and start the Secure copying of application databases task:

1. In the Application Console tree, in the context menu of the **Update** node, select **Start secure copying of databases**.

   The welcome window of the secure application databases copy wizard opens.
2. Click **Next >**.
3. Under **Update source**, select an update source:

   - **Kaspersky Security Center Administration Server**.

     You can only select this option if Kaspersky applications on your network are administered using the Kaspersky Security Center remote access system and if Network Agent (the Kaspersky Security Center component that provides the connection between protected devices and Administration Server) is installed on the protected device.

     This option is selected by default.
   - **Kaspersky update servers**.

     Kaspersky HTTP and HTTPS servers from which Kaspersky applications download database and application module updates.
   - **Custom HTTP or FTP servers, or network folders**.
4. If at the previous step you selected **Kaspersky Security Center Administration Server**, configure the **Use Kaspersky update servers if specified servers are not available** functionality. If this option is enabled, Kaspersky Industrial CyberSecurity for Nodes will use Kaspersky update servers as an update source if the Kaspersky Security Center Administration Server is unavailable.

5. Under **Update source connection settings**, configure the use of a proxy server for connecting to update sources.

6. Click **Next >**.

7. From the drop-down list, choose the connected secure Rutoken removable drive where you want to save the application anti-virus databases.

   You cannot use the same Rutoken removable drive simultaneously for creating Portable Auditor and for securely copying application databases.

   Only a Rutoken removable drive that has been specifically authorized through a rule of the Device Control component can be used as a secure removable drive.

8. Under **Security settings**, in the **Enter the current administrator PIN code** field, enter the administrator PIN code set on the Rutoken removable drive to protect its contents from being read, copied, or written by potential intruders.

9. To change the current administrator PIN code:

   a. Select the **Change the current administrator PIN code (only digits and Latin symbols are allowed)** check box.

   b. Enter the new PIN.

   c. Confirm the new PIN.

10. Set a user PIN. This PIN will be required by the employee who will update the application databases using the *Secure update of application databases* task and the selected Rutoken removable drive:

    a. Enter the user PIN.

    b. Confirm the user PIN.

11. Click **Next >**.

Secure copying of application databases to the Rutoken removable drive is started. The settings are saved and applied while the task is running.

It is not recommended to connect two Rutoken removable drives to the same device and simultaneously running the Secure copying of application databases and Creating Portable Auditor tasks. In this case, the tasks may end with an error.

Secure update of application databases

The *Secure update of application databases* task is necessary to update the application databases using a secure removable drive protected from reading, copying, and writing by potential intruders, in a closed corporate network and on devices that do not have access to the application databases.

This task can only be started via the Application Console installed on the same device as Kaspersky Industrial CyberSecurity for Nodes. Configuring the task in the Administration Console or Web Console is not possible.

To run the Secure update of application databases task:

1. In the Application Console tree, in the context menu of the **Update** node, select **Start secure update of databases**.

   The welcome window of the secure application database update wizard opens. Click the **Next >** button.

2. From the drop-down list, choose the connected secure removable drive containing the application anti-virus databases.

   Only a Rutoken removable drive that has been specifically authorized through a rule of the Device Control component can be used as a secure removable drive.

3. Enter the PIN for the Rutoken removable drive, specified during the application database copying step.

4. Click **Finish**.

The secure update of application databases task starts. The application databases will be copied from the Rutoken removable drive.

Rolling back Kaspersky Industrial CyberSecurity for Nodes database updates

Before database updates are performed, Kaspersky Industrial CyberSecurity for Nodes creates backup copies of the previously used databases. If an update is interrupted or results in an error, Kaspersky Industrial CyberSecurity for Nodes will automatically return to using the previously installed databases.

If any problems arise after you have updated the databases, you can roll back to the previously installed updates through the *Last update rollback* task.

To run the Last update rollback task:

1. In the Application Console tree, open the **Update** → **Last update rollback** section.

2. In the results pane, click the **Start** link.

Update task statistics

While the Update task is running, the real-time information is displayed about the amount of data downloaded since the task started, as well as other task execution statistics.

When the task is complete or stopped, the information is available in the task log.

To view the Update task statistics:

In the Application Console tree, open the **Update** → **Update of databases and application modules** section.

The results panel, under **Statistics**, you can find information about the total amount of obtained data.

Detection and Response solutions

Kaspersky Detection and Response solutions are security systems for detecting advanced threats and indicators of attack on different levels of an organization's infrastructure. Detection and Response solutions provide information about the detected threat and allow managing Threat Response actions.

Thus, Detection and Response solution do the following:

- Receive information about the operation of a computer, server, or other devices (telemetry).
- Automatically analyze the information to detect threats.
- Generate alert details as columns of the threat development chain for analysis and choosing Threat Response actions.
- Carry out Threat Response actions (for example, network isolation of the computer).

Kaspersky Industrial CyberSecurity for Nodes supports Detection and Response solutions using the *Endpoint Agent* built-in agent (hereinafter also referred to as *built-in agent*). The built-in agent sends telemetry to servers of solutions and carries out Threat Response actions. The built-in agent supports:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response
- Kaspersky Endpoint Detection and Response Expert (on-premise)
- Kaspersky Anti Targeted Attack Platform (telemetry only)

Kaspersky Industrial CyberSecurity Endpoint Detection and Response

Kaspersky Industrial CyberSecurity Endpoint Detection and Response is a solution designed to protect an organization IT infrastructure from complex cyberthreats. The solution's functionality combines automatic threat detection with threat response capabilities to resist complex attacks, including new exploits, ransomware, fileless attacks, and methods that use legitimate system tools.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response reviews and analyses the development of threats and provides the Security Officer or Administrator with information about a potential attacks in order to respond to the threat in a timely manner or automatically performs the specified response actions.

Users with a Kaspersky Security for Business Professional license have access to Kaspersky Industrial CyberSecurity Endpoint Detection and Response additional functionality, which expands analysis and response capabilities:

- Sending a file from Quarantine to Kaspersky TIP
- Response actions for Active Directory users from alert details
- Assigning Kaspersky ASAP training courses to users from alert details

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the solution in the U.S.

Solution architecture

Kaspersky Industrial CyberSecurity Endpoint Detection and Response includes the following components:

- An EPP Kaspersky application (Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes) that supports Kaspersky Industrial CyberSecurity Endpoint Detection and Response functionality and is installed on separate devices in the organization IT infrastructure. This application continuously monitors processes running on protected devices, open network connections, and file changes.
- Kaspersky Endpoint Agent is an application that continuously monitors and sends information about processes, open network connections, and modified files on the device to Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0. You don't have to install Kaspersky Endpoint Agent if you are using Kaspersky Industrial CyberSecurity for Linux Nodes or Kaspersky Industrial CyberSecurity for Nodes version 4.5 and later.
- A solution for centralized network security management (Kaspersky Security Center).
- Threat Intelligence Tools:
  - Kaspersky Security Network (KSN) infrastructure of cloud services, which provides access to the online Kaspersky Knowledge Base, which contains information about the reputation of files, web resources, and software. Using data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.
  - Integration with Kaspersky Private Security Network (KPSN) that allows the users to access KSN reputation databases, as well as other statistics without submitting data to KSN from their devices.
  - Integration with Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and URLs. Integration with Kaspersky Threat Intelligence Portal allows you to:
    - Search for additional information about objects in the alert details.
    - Send a quarantined file for threat analysis (when using the extended capabilities of Kaspersky Industrial CyberSecurity Endpoint Detection and Response).
  - Kaspersky Threats database.

Multitenancy

Multitenancy is an operation mode when the solution is used to protect infrastructure of several organizations at the same time.

You can use Kaspersky Industrial CyberSecurity Endpoint Detection and Response to protect infrastructure of several organizations at the same time using Kaspersky Security Center. For this purpose create virtual Administration Servers for the organizations which you want to protect using Kaspersky Industrial CyberSecurity Endpoint Detection and Response. These virtual Administration Servers must be created under the physical Administration Server of the provider organization. For details on creating virtual Administration Servers, refer to the Kaspersky Security Center Help.

A separate virtual Administration Server must be created for each tenant organization. The administrator of a physical Administration Server can manage the solution on all devices that are managed by this Server. The administrator of the virtual Administration Server can manage the solution only on the devices connected to the Server that he administers.

Compatibility with Kaspersky applications

Kaspersky Industrial CyberSecurity Endpoint Detection and Response is compatible with the following versions of Kaspersky applications:

- Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 and later.

  Kaspersky Industrial CyberSecurity for Linux® Nodes requires the following versions of Kaspersky Security Center:

  - Kaspersky Security Center Windows 14.2 and later.
  - Kaspersky Security Center Linux 15.1 and later.

- Kaspersky Industrial CyberSecurity for Nodes 3.1 and later.

  When using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0, Kaspersky Industrial CyberSecurity for Nodes also requires installation of Kaspersky Endpoint Agent. Kaspersky Endpoint Agent can be installed on individual devices in the organization IT infrastructure that have Microsoft® Windows® operating system. The application provides support for Kaspersky Industrial CyberSecurity Endpoint Detection and Response for Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity Endpoint Detection and Response supports integration with Kaspersky Endpoint Agent 3.13 and later.

  Kaspersky Industrial CyberSecurity for Nodes 4.5 and later introduces the built-in agent for working within the Kaspersky Industrial CyberSecurity Endpoint Detection and Response solution.

  The following versions of Kaspersky Security Center must be used with the specified versions of Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent:

  - Kaspersky Security Center versions from 10.5 to 12.1 support the limited functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response (you can find out more about the functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response with different versions of Kaspersky Security Center from the Kaspersky partner you purchased the license from).
  - Kaspersky Security Center Windows 12.1 and later has full support of Kaspersky Industrial CyberSecurity Endpoint Detection and Response functionality.
  - Kaspersky Security Center Linux 15.1 and later.

The extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response for users with a Kaspersky Security for Business Professional license is compatible with the following versions of Kaspersky applications:

- Kaspersky Industrial CyberSecurity for Nodes 4.5 and later.
- Kaspersky Security Center Linux version 15.4 and later, with the Endpoint Detection and Response plug-in version 15.4 and later installed.

Deployment and initial setup

The following conditions must be met for Kaspersky Industrial CyberSecurity Endpoint Detection and Response to work:

- A supported version of Kaspersky Security Center with the Web Console is installed.

  For more details on installing Kaspersky Security Center, see the Kaspersky Security Center Help and Kaspersky Security Center Linux Help.

- Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes is installed on the protected devices (for information on installing Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Industrial CyberSecurity for Linux Nodes Help).

- The Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes management web plug-in has been installed.

  For detailed information about installing management web plug-ins, refer to the Kaspersky Security Center Help.

- The Endpoint Detection and Response web plug-in is installed.

Deployment and initial setup of the solution using Kaspersky Industrial CyberSecurity for Nodes 4.5 and later.

The deployment and initial configuration scenario consists of the following steps:

1. **Installing the Endpoint Detection and Response (Industrial CyberSecurity) component**

   In installation package settings or in the Setup Wizard, or by changing the set of application components in the Windows Control Panel, at the step when you must select application components for installation, select the following: **Full functionality → Endpoint Agent → Endpoint Detection and Response (Industrial CyberSecurity)**.

   > To finish changing the set of application components, you must restart the computer.

2. Activating Kaspersky Industrial CyberSecurity Endpoint Detection and Response
3. **Enabling the required components of Kaspersky Industrial CyberSecurity for Nodes**

Make sure that the following components of Kaspersky Industrial CyberSecurity for Nodes are enabled and running:

- Real-Time File Protection
- Exploit Prevention
- Anti-Cryptor
- Remediation Engine

4. **Enabling and configuring the Endpoint Detection and Response (Industrial CyberSecurity) component**

   How to enable and configure Endpoint Detection and Response (Industrial CyberSecurity) component in the Kaspersky Security Center Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

      The policy properties window opens.
   3. Select the **Application settings** tab.
   4. Select the **Telemetry collection servers** section.
   5. In the **Endpoint Detection and Response (Industrial CyberSecurity)** block, click the **Settings** button.

      The **Endpoint Detection and Response (Industrial CyberSecurity)** window opens.
   6. Select the **Enable Endpoint Detection and Response (Industrial CyberSecurity)** check box.
   7. Configure Network isolation settings.
   8. Configure Execution prevention settings.
   9. If necessary, enable the counter for threats detected by Cloud Sandbox using the toggle with the same name.
   10. Save your changes.

   For information on enabling and configuring the Kaspersky Industrial CyberSecurity Endpoint Detection and Response integration in Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

5. **Enabling data transfer to Kaspersky Security Center Administration Server**

   To enable all the Kaspersky Industrial CyberSecurity Endpoint Detection and Response features, data transfer must be enabled for the following types of data:

   - Quarantine file data.

     In Kaspersky Security Center Web Console you can download files from quarantine for analysis.
   - Threat development chain data.

     You can view alert details and take response actions in Web Console.

How to enable data transfer to the Administration Server in Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Go to the **Logs and notifications** section.
5. In the **Interaction with Administration Server** block, click the **Settings** button.
6. In the window that opens, select the following check boxes:
   - **Quarantine files**.
   - **Threat development chain**.
7. Save your changes.

For the Kaspersky Industrial CyberSecurity Endpoint Detection and Response solution to work with Administration Server via Kaspersky Security Center Web Console, you must establish a new secure connection, a *background connection*.

Establishing a background connection in Web Console

1. In the main window of the Web Console, select **Settings** → **Integration**.
2. Go to the **Integration** section.
3. Turn on the **Background connection for integration Enabled** toggle.
4. Save your changes.

6. **Configuring threat report**

   Configure the threat report for viewing incident cards.

7. **Adding a widget**

   Add the EDR alerts widget to the dashboard for monitoring alerts.

8. **Displaying the list of alerts**

   Enable display of the Alerts section in Kaspersky Security Center Web Console.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response is ready for use.

Deployment and initial setup of the solution using Kaspersky Industrial CyberSecurity for Nodes versions 3.1–4.0

When using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0, you must additionally install and activate Kaspersky Endpoint Agent on the protected device, install the Kaspersky Endpoint Agent management web plug-in, and create a corresponding policy. For more details, refer to the Kaspersky Endpoint Agent Help.

Deployment and initial setup of the solution using Kaspersky Industrial CyberSecurity for Linux Nodes

For information on enabling and configuring the Kaspersky Industrial CyberSecurity Endpoint Detection and Response integration in Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Solution activation

Activating Kaspersky Industrial CyberSecurity Endpoint Detection and Response involves activating the following applications:

- Kaspersky Industrial CyberSecurity for Nodes.

  When using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0, Kaspersky Endpoint Agent must also be activated.

- Kaspersky Industrial CyberSecurity for Linux Nodes.

These applications must be installed on the protected devices and activated using a license that includes Kaspersky Industrial CyberSecurity Endpoint Detection and Response functionality.

You can purchase the license for Kaspersky Industrial CyberSecurity Endpoint Detection and Response in the following ways:

- As part of a license to use Kaspersky Industrial CyberSecurity for Nodes.

  In this case, Kaspersky Industrial CyberSecurity Endpoint Detection and Response will become available after you complete the initial setup of the solution.

- Separately, in addition to the previously purchased license to use Kaspersky Industrial CyberSecurity for Nodes.

  If you purchased a license to use Kaspersky Industrial CyberSecurity Endpoint Detection and Response separately, after installing and activating the Kaspersky Industrial CyberSecurity for Nodes application on your devices, you must activate Kaspersky Industrial CyberSecurity for Nodes (when using application versions 3.1 to 4.0, Kaspersky Endpoint Agent must also be activated) using a new activation code or key file.

After activating the application, perform the initial setup of the solution.

Activating the extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response involves activating Kaspersky Security Center Linux under a Kaspersky Security for Business Professional license.

You can purchase a Kaspersky Security for Business Professional license to use the extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response in the following ways:

- As part of a license to use EPP applications and Kaspersky Security Center.

  In this case, the solution will become available after you complete the initial setup of the solution.

- Separately, in addition to the previously purchased license to use Kaspersky Security Center.

  If you purchased a Kaspersky Security for Business Professional license separately, after installing and activating Kaspersky applications on your devices, you must reactivate Kaspersky Security Center Linux using a new activation code or key file. After that, perform the initial setup of the solution.

For more information on activating the solution, see the Kaspersky application Help:

- Kaspersky Security Center.
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Endpoint Agent

Configuring threat report for viewing alert details

To configure the capability to open the alert details window from the threat report:

1. In the main window of the Web Console, select **Monitoring** → **Reports**.
2. In the list of reports, select the check box next to the **Report on threats** template report and click the **Open report template properties** button.
3. In the report properties window that opens, go to the **Fields** tab.
4. Make sure that the **Open alert** field is available in the list of report fields in the **Details fields** settings block.
5. If the **Open alert** field is not available in the list, follow these steps:
   a. Click **Add**.
   b. At the right side of the window, select the **Open alert** field from the drop-down list.
   c. Click **OK**.
6. Click **Save**.

Adding EDR alerts widget

The EDR alerts widget displays information about the number of alerts on the devices for the last month. The widget is available on the **Dashboard** tab in Kaspersky Security Center Web Console. The widget allows you to switch to the **Alerts** section, where a list of alerts on devices is displayed.

To add the EDR alerts widget to the dashboard:

1. Go to **Monitoring** → **Dashboard**.
2. Click the **Add or restore web widget** button.
3. In the list of available widgets, select the **Alerts** widget from the **Threat statistics** category.
4. Click the **Add** button.
   The web widget is added to the end of the dashboard.

For more details on working with widgets, please refer to the Kaspersky Security Center Help.

Monitoring the solution performance on devices

Kaspersky Security Center functionality allows you to get information on the current protection status of the devices and on the devices in your infrastructure where the EPP application that supports Kaspersky Industrial CyberSecurity Endpoint Detection and Response is not installed.

You can get this information by generating a selection of devices by the status of Kaspersky Industrial CyberSecurity Endpoint Detection and Response component.

To generate a device selection:

1. In Kaspersky Security Center Web Console, go to the **Asset management** → **Device selections** section.
2. Create a new device selection with the following condition:
   a. Select the **Details of Kaspersky applications** section.
   b. In the **Application components** list, select one of the following options:
      - The **Endpoint Detection and Response (Industrial CyberSecurity)** component for Kaspersky Industrial CyberSecurity for Nodes version 4.5 or later.
      - The **Endpoint Detection and Response Optimum** component for Kaspersky Endpoint Agent (if Kaspersky Industrial CyberSecurity for Nodes version 3.1 to 4.0 is installed on the device).
      - The **Kaspersky Industrial CyberSecurity Endpoint Detection and Response Integration** component for Kaspersky Industrial CyberSecurity for Linux Nodes.
   c. In the **Status** drop-down list, select the required value of the selection criterion to display devices with this operation status.
   d. Click **Save**.

The new selection displays the list of devices with the selected operation status of Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Upgrading to Kaspersky Industrial CyberSecurity Endpoint Detection and Response with extended functionality

If you have purchased a Kaspersky Security for Business Professional license, you can use Kaspersky Industrial CyberSecurity Endpoint Detection and Response with extended functionality.

Upgrading to Kaspersky Industrial CyberSecurity Endpoint Detection and Response with extended functionality includes the following steps:

1. **Updating Kaspersky Security Center Linux to version 15.4 or later, including Network Agent components on user computers and Kaspersky Security Center Web Console for Linux**

   See Kaspersky Security Center Help for more details.

2. **Updating EPP applications on protected devices to a version that supports Kaspersky Industrial CyberSecurity Endpoint Detection and Response with extended functionality**

3. **Installing the Endpoint Detection and Response web plug-in version 15.4 or later in Kaspersky Security Center**

   For more details on installing plug-ins, refer to the Kaspersky Security Center Help.

4. **Activating the solution under a Kaspersky Security for Business Professional license**

5. **Configuring integration with Active Directory for threat response**

   For more details on configuring the integration, refer to the Kaspersky Security Center Help.

6. **Configuring integration with Kaspersky Automated Security Awareness Platform for threat response**

   For more details on configuring the integration, refer to the Kaspersky Security Center Help.

7. **Configuring integration with Kaspersky Threat Intelligence Portal for threat response**

   For more details on configuring the integration, refer to the Kaspersky Security Center Help.

Response actions

This section contains information on the response actions to the detected threats that are available in Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Network isolation of a device

Kaspersky Industrial CyberSecurity Endpoint Detection and Response provides the ability to isolate devices from the network on demand (manually) or as an automatic action to respond to detected threats.

In case of automatic response, the corresponding commands will be executed on the devices without confirmation from the operator. Despite the use of standard operating system mechanisms, unforeseen problems may occur. They can be caused by incorrect or highly-focused configuration of devices, compatibility problems, or errors in the software of devices or industrial-control systems (ICS), which do not appear during normal use. For example, the following problems may occur: turning off the device, loss of communication with the device, inoperability of the device, other failures in the operation of the solution and equipment. Also, unintentional impact on the ICS operation is possible.

The administrator of Kaspersky Industrial CyberSecurity Endpoint Detection and Response is fully responsible for the impact of automatic actions of the solution in relation to detected threats on the stability of the ICS and the technological process.

After enabling network isolation, the application breaks all active TCP/IP connections and blocks all new TCP/IP network connections on the devices, except for the connections listed below:

- Connections specified as network isolation exclusions
- Connections initiated by services of Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes
- Connections initiated by the Kaspersky Security Center Network Agent

You can manage network isolation from the Web Console.

Options when working with network isolation

The following options are available when working with network isolation:

- Automatically enabling network isolation upon detection of an IOC.
- Manually enabling network isolation for a device.
- Enabling network isolation from the alert details card.
- Manually disabling network isolation for a device.
- Configuring the network isolation interval using the Kaspersky Industrial CyberSecurity policy.
- Configuring the network isolation interval for a device.

Automatic Network isolation mode

You can configure Network isolation to be turned on automatically in response to an IOC detection. You can configure the automatic Network isolation mode with a group policy.

How to configure Network isolation to be turned on automatically in response to an IOC detection

1. In the main window of the Web Console, select **Asset management** → **Tasks**.

   The list of tasks opens.

2. Click the Kaspersky Industrial CyberSecurity for Nodes **IOC Scan** task.

   The task properties window opens.

   If necessary, create the *IOC Scan* task.

3. Select the **Application settings** tab.

4. In the **Action on IOC detection** block, select the **Take response actions after an IOC is found** and **Isolate computer from the network** check boxes.

5. Save your changes.

As a result, when an IOC is detected, the application isolates the computer from the network to prevent the threat from spreading.

You can configure automatic Network isolation to be disabled after a certain period of time. By default, the application turns off Network isolation after 8 hours have passed from the time when it was turned on. You can also turn off Network isolation manually (see the instructions below). After turning off network isolation, the computer can use the Network without restrictions.

How to configure the delay for turning off Network isolation of a computer in automatic mode

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Telemetry collection servers** → **Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.
5. In the **Network isolation** block, click **Configure computer unlock settings**.
6. This opens a window; in this window, select the **Automatically unlock isolated computer in** check box and enter the delay for automatically turning off Network isolation.
7. Save your changes.

Manual Network isolation mode

You can manually turn Network isolation on and off. You can configure the manual Network isolation mode using the computer properties in the Kaspersky Security Center Administration Console.

You can enable Network isolation in the following ways:

- In alert details.
- Using local application settings.

How to turn on Network isolation of a computer manually

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
2. Select the computer for which you want to configure local application settings.

   This opens the computer properties.
3. Select the **Application** tab.
4. Click **Kaspersky Industrial CyberSecurity for Nodes**.

   This opens the local application settings.
5. Select the **Application settings** tab.

6. Go to **Telemetry collection servers → Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.

7. Under **Network isolation**, click the **Isolate computer from the network** button.

8. Click **OK**.

You can configure automatic Network isolation to be disabled after a certain period of time. By default, the application turns off Network isolation after 8 hours have passed from the time when it was turned on. After turning off network isolation, the computer can use the Network without restrictions.

How to configure the delay for turning off Network isolation of a computer in manual mode

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.

2. Select the computer for which you want to configure local application settings.

   This opens the computer properties.

3. Select the **Tasks** tab.

   This displays the list of tasks available on the computer.

4. Select the **Network isolation** task.

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

6. This opens a window; in this window, select the delay for turning off Network isolation.

7. Save your changes.

How to turn off Network isolation of a computer manually

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.

2. Select the computer for which you want to configure local application settings.

   This opens the computer properties.

3. Select the **Application** tab.

4. Click **Kaspersky Industrial CyberSecurity for Nodes**.

   This opens the local application settings.

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

6. Go to **Telemetry collection servers → Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.

7. Under **Network isolation**, click the **Unblock computer isolated from the network** button.

8. Save your changes.

You can also disable Network isolation locally on the command line.

Network isolation exclusions

You can configure Network isolation exclusions. Network connections that match the rules are not blocked on the computer when Network isolation is turned on.

To configure Network isolation exclusions, you can use a list of standard network profiles. By default, exclusions include network profiles containing rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles. You can also modify the settings of standard network profiles or define exclusions manually (see instructions below).

Exclusions specified in policy properties are applied only if Network isolation is turned on automatically in response to a detected threat. Exclusions specified in computer properties are applied only if Network isolation is turned on manually in computer properties in the Kaspersky Security Center console or in alert details.

An active policy does not prevent applying exclusions from Network isolation configured in computer properties because these parameters have different usage scenarios.

How to add a Network isolation exclusion in automatic mode

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Telemetry collection servers** → **Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.
5. In the **Network isolation exclusions** block, click **Exclusions**.
6. This opens a window; in this window, click **Add from profile** and select standard network profiles for configuring exclusions.

   Network isolation exclusions from the profile are added to the list of Network isolation exclusions. You can view the properties of network connections. If necessary, you can modify network connection settings.
7. If necessary, add a Network isolation exclusion manually. To do so, in the window with the list of exclusions, click **Add** and manually edit network connection settings.
8. Save your changes.

How to add a Network isolation exclusion in manual mode

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
2. Select the computer for which you want to configure local application settings.

   This opens the computer properties.

3. Select the **Tasks** tab.

   This displays the list of tasks available on the computer.

4. Select the **Network isolation** task.

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

6. This opens a window; in this window, click **Exclusions**.

7. This opens a window; in this window, click **Add from profile** and select standard network profiles for configuring exclusions.

   Network isolation exclusions from the profile are added to the list of Network isolation exclusions. You can view the properties of network connections. If necessary, you can modify network connection settings.

8. If necessary, add a Network isolation exclusion manually. To do so, in the window with the list of exclusions, click **Add** and manually edit network connection settings.

9. Save your changes.

You can also view the Network isolation exclusion list locally using the command line. In this case, the computer must be isolated.

Tag for isolated devices

The ISOLATED FROM NETWORK tag is added to all isolated devices. This tag cannot be removed while the device is isolated.

> If you add this tag manually, the device will not be isolated from the network.

The ISOLATED FROM NETWORK tag allows you to detect isolated devices. For more details, see the Viewing a list of isolated devices section.

For details on managing network isolation in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

IOC Scan

An *Indicator of Compromise (IOC)* is a set of data about an object or activity that indicates unauthorized access to a device (compromised data). For example, many unsuccessful attempts to sign in to the system can constitute an Indicator of Compromise.

IOC files are used to search for IOCs. IOC files contain a set of indicators that are compared to the indicators of an event. If the compared indicators match, the EPP application considers the event to be alert.

Kaspersky Industrial CyberSecurity for Nodes includes the *IOC Scan* task, which is a group or local task that uses IOC files. In case of a match indicators of compromise, the application performs the action specified in the properties of the *IOC Scan* task. The following response actions are available for the detected IOCs:

- Isolate device from the network.
- Run critical areas scan.
- Move the copy of the object to the quarantine, and delete the object.

You can create the *IOC Scan* task in the following ways:

- From alert details.
- **In the Web Console.**

  1. In the main window of the Web Console, select **Asset management** → **Tasks**.

     The list of tasks opens.

  2. Click **Add**.

     The Task Wizard starts.

  3. Configure the task settings:

     a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.

     b. In the **Task type** drop-down list, select **IOC Scan**.

     c. If necessary, edit the task name in the **Task name** field.

     d. In the **Devices to which the task will be assigned** block, select the task scope.

  4. Select devices according to the selected task scope option.

  5. Enter the account credentials of the user whose rights you want to use to run the task.

     > By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).

     The system account (SYSTEM) does not have permission to perform the *IOC Scan* task on network drives. If you want to run the task for a network drive, select the account of a user that has access to that drive.

  6. Finish the wizard.

     The created task is displayed in the list of tasks.

  7. Click the name of the created task.

     The task properties window opens.

  8. Select the **Application settings** tab.

  9. Go to the **IOC Scan settings** section.

10. Upload the IOC files to search for indicators of compromise.

    We do not recommend adding or removing IOC files after starting the task. This can cause the IOC scan results to display incorrectly for prior runs of the task. To search for indicators of compromise with new IOC files, we recommend adding new tasks.

11. If necessary, configure Retrospective IOC Scan. In this mode of the *IOC Scan* task, Kaspersky Industrial CyberSecurity for Nodes searches for indicators of compromise in data of protected devices received over the specified period of time. The application analyzes data in operating system logs and browser logs installed on the protected computer.

    To start the task in *Retrospective IOC Scan* mode, the uploaded IOC files must include one of or more terms from this list: *FileItem/**, *Network/**, *PortItem/**, *ProcessItem/**, *RegistryItem/**, *UrlHistoryItem/**.

    Do the following:

    a. Select the **Enable Retrospective IOC Scan** check box.

    b. Specify the time period for the search in days. The maximum value is 14 days.

    While running the task, the application analyzes information collected for the specified period, starting from the time when the task was started.

    The default setting is 1 day.

    c. In the **Advanced** section of task properties, make sure that check boxes are selected for all data types mentioned in the uploaded IOC file.

    d. If the uploaded IOC file contains an indicator of compromise with the *Network/** term, select the check box next to the *Network data - NetworkItem* data type, which is cleared by default.

    The *IOC Scan* task starts in the retrospective scanning mode. In this mode, for each file, the application publishes normal task results and retrospective IOC scan results.

    Kaspersky Industrial CyberSecurity for Nodes displays the PID and UPID fields only for retrospective scan results. Also, if extended telemetry is disabled, retrospective IOC scanning has the following limitations:

    - The application does not populate the Created, Modified, Changed, Accessed, FileAttributes fields for FileItem records.
    - For existing files that have not been executed, the Md5sum, Sha256sum, SizeInBytes fields in retroscan results are set to 0.
    - For detected files that have been deleted, the application does not compute a hash.

12. If necessary, configure the actions to be performed by Kaspersky Industrial CyberSecurity for Nodes when it detects an indicator of compromise:

    a. Select the **Take response actions after an IOC is found** check box.

    b. Select check box next to the actions to be performed by Kaspersky Industrial CyberSecurity for Nodes when it detects an indicator of compromise:

    - **Isolate computer from the network**. If this option is selected, Kaspersky Industrial CyberSecurity for Nodes isolates the computer from the network to prevent the threat from spreading. You can configure the duration of the isolation in Endpoint Detection and Response (KSC) component settings.
    - **Move copy to Quarantine, delete object**. If this option is selected, Kaspersky Industrial CyberSecurity for Nodes deletes the malicious object found on the computer. Before deleting an object, Kaspersky Industrial CyberSecurity for Nodes creates a backup copy and places it in quarantine.
    - **Run Critical Areas Scan**. If this option is selected, Kaspersky Industrial CyberSecurity for Nodes runs the predefined task: *Critical Areas Scan*.

13. Go to the **Advanced** section.

14. Select data types (IOC documents) that must be analyzed as part of the task.

    Kaspersky Industrial CyberSecurity for Nodes automatically selects data types (IOC documents) for the *IOC Scan* task in accordance with the content of loaded IOC files. We do not recommend clearing the selection of data types on your own.

    For the *Windows registry - RegistryItem* data type, Kaspersky Industrial CyberSecurity for Nodes analyses a predefined set of registry keys.

15. If necessary, specify additional settings for the Files - FileItem data type:

    a. Click **IOC documents**.

    The **File scan settings - FileItem** window opens.

    b. Under **Search for IOC in the following areas**, select data that you want to be analyzed by the task.

    c. Under **Scan custom areas**, select areas on disks of the protected device in which you want to look for indicators for compromise.

    By default, Kaspersky Industrial CyberSecurity for Nodes scans for IOCs only in important areas of the computer, such as the Downloads folder, the desktop, the folder with temporary operating system files, etc. You can specify your own paths to the areas that you need.

    d. Click **OK**.

16. If necessary, specify additional settings for the Windows event logs - EventLogItem data type:

    a. Click **Logs and dates**.

    The **Windows event log scan settings - EventLogItem** window opens.

    b. To have the task ignore events that were registered before a certain moment, select the **Scan only events that are logged within the specified period** check box and specify the date and time.

c. Under **Scan events that belong to the following channels**, select Windows event logs you want to be analyzed by the task.

d. Click **OK**.

For the EventLogItem\source IOC term, use the **Provider Name** value from the XML schema of the event.

17. Configure the task start schedule on the **Schedule** tab.

18. Save your changes.

19. Select the check box next to the task.

20. Click **Start**.

- Using the command line.

You can view the results of the task in task properties in the **Results** section. You can view the information about detected indicators of compromise in the task properties: **Application settings** → **IOC Scan results**.

Kaspersky Industrial CyberSecurity for Nodes looks for duplicates among records created for the same IOC file and keeps only unique records in task results. Duplicates are records of the same type that have the same values of all compared fields. The application also may not create a record if it lacks a value in **one or more fields**.

Type	Compared fields	Condition for not creating a record
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Missing values of the FullPath, Md5sum, Sha256sum fields. • Missing values of the FullPath field and identical values of the Md5sum, Sha256sum fields.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Missing value of at least one of the following fields: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Missing value of the startTime or PID field.

The **Alert Details** window may display RegistryItem records with identical field values. Such records are not duplicates because they have different values of the Text field, which is not displayed in the interface.

IOC scan results are kept for 30 days. After this period, Kaspersky Industrial CyberSecurity for Nodes automatically deletes the oldest entries.

An IOC scan is ended after finding 128 matches with indicators of compromise described in IOC files. This is necessary to limit the number of entries in the *IOC Scan* task report to make analysis easier and to prevent the report from becoming too big because of imprecisely formulated indicators of compromise that can produce an extraordinary number of matches.

For more details on creating an IOC Scan task in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

IOC file requirements

When creating IOC Scan tasks, consider the following IOC file-related requirements and limitations:

- The application supports IOC files with the IOC and XML extensions in the open standard OpenIOC versions 1.0 and 1.1 for describing indicators of compromise.
- After uploading IOC files, you can manually edit the files in the built-in editor directly in task properties. Kaspersky Industrial CyberSecurity for Nodes supports changing the content of IOC files that comply with OpenIOC version 1.1. It is not possible to modify the content of IOC files compliant with OpenIOC version 1.0.
- If, when creating an *IOC Scan* task on the command line, you upload IOC files, some of which are not supported, when the task is run, the application uses only the supported IOC files. If, when creating an *IOC Scan* task on the command line, all of the IOC files that you upload turn out to be unsupported, the task can still be run, but it will not detect any indicators of compromise. It is not possible to upload unsupported IOC files using Web Console or Cloud Console.
- Semantic errors and unsupported IOC terms and tags in IOC files do not cause task execution to fail. In such sections of IOC files, the application detects no match.
- The identifiers of all IOC files used in a single IOC Scan task must be unique. If there are IOC files with the same identifier, it might affect the task execution results.
- A single IOC file must not exceed 2 MB in size. Using larger files will cause IOC Scan tasks to terminate with an error. The total size of all files added to the IOC collection should not exceed 10 MB. If the total size of all files exceeds 10 MB, you need to split the IOC collection and create multiple IOC Scan tasks.
- It is recommended to create one IOC file per threat. This makes it easier to analyze the results of the *IOC Scan* task.

The file that you can download by clicking the link below, contains a table with the full list of IOC terms of the OpenIOC standard.

DOWNLOAD THE IOC_TERMS.XLSX FILE

Features and limitations of the application's support for the OpenIOC standard are shown in the following table.

Features and limitations of support for OpenIOC version 1.0 and 1.1.

Supported conditions	OpenIOC 1.0:
	
	`is`
	`isnot` (as an exception from the set)
	`contains`
	`containsnot` (as an exception from the set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Supported condition attributes	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Supported operators	`AND` `OR`
Supported data types	`"date"`: date (applicable conditions: `is`, `greater-than`, `less-than`) `"int"`: integer (applicable conditions: `is`, `greater-than`, `less-than`) `"string"`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duration in seconds (applicable conditions: `is`, `greater-than`, `less-than`)

Features of data type interpretation	The `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` and `"base64Binary"` data types are interpreted as string.
	
	The application supports interpretation of the `Content` setting for the `int` and `date` data types when it is set in the form of intervals:
	
	OpenIOC 1.0:
	Using the `TO` operator in the `Content` field:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Using the `greater-than` and `less-than` conditions
	Using the `TO` operator in the `Content` field
	The application supports interpretation of the `date` and `duration` data types if the indicators are set in `ISO 8601, Zulu time zone, UTC` format.

Extended telemetry for IOC Scan

We recommend enabling extended telemetry on the computer for retrospective IOC scanning. Extended telemetry improves the accuracy of IOC detection, but uses more resources of the computer.

Extended telemetry includes the support of the following additional terms:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

If extended telemetry is disabled, Kaspersky Industrial CyberSecurity for Nodes may rotate the information about detected indicators of compromise.

To enable extended telemetry:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Telemetry collection servers** → **Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.
5. Select the **Enable advanced system activity logging** check box.
6. Save your changes.

IOC scan scope in the registry (RegistryItem)

When you add the RegistryItem data type to the IOC scan scope, Kaspersky Industrial CyberSecurity for Nodes scans the following registry keys:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile
```

```
HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Running Critical Areas Scan

One of the possible response actions when a threat is detected is running Critical Areas scan on the device.

You can run Critical Areas scan manually or configure the scan to run automatically as a result of alert response actions.

For more details on Critical Areas Scan in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Execution prevention

Execution prevention allows managing the running of executable files and scripts, as well as opening office format files. In this way, you can, for example, prevent the execution of applications that you consider insecure. As a result, the spreading of the threat can be stopped. Execution prevention supports **a set of office file extensions** and **a set of script interpreters**.

Execution prevention supports the following script interpreters:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe

- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Execution prevention supports working with Java applications in the Java runtime environment (java.exe and javaw.exe processes).

Kaspersky Industrial CyberSecurity for Nodes supports preventing the opening of office format files in certain applications. The information about supported file extensions and applications is listed in the following table.

Supported file extensions for Execution prevention

Application name	Executable file	File extension
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Execution prevention rule

Execution prevention manages user access to files with execution prevention rules. *Execution prevention rule* is a set of criteria that the application takes into account when reacting to an object execution, for example when blocking object execution. The application identifies files by their paths or checksums calculated using MD5 and SHA256 hashing algorithms.

You can create Execution prevention rules:

- In alert details.

  This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

- Using a group policy or local application settings.

  You must enter the file path or hash (SHA256 or MD5), or both the file path and the file hash.

Execution prevention has the following limitations:

1. Prevention rules do not cover files on CDs or in ISO images. The application does not block execution or opening of these files.
2. It is impossible to block the startup of system-critical objects (SCO). SCOs are files that the operating system and the Kaspersky Industrial CyberSecurity for Nodes application require to be able to run.
3. It is not recommended to create more than 5000 run prevention rules, as this can cause system instability.

Execution prevention rule modes

Execution prevention can work in two modes:

- **Inform**

  In this mode, Kaspersky Industrial CyberSecurity for Nodes publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Windows event log and Kaspersky Security Center, but does not block the attempt to run or open the object or document. By default, the mode is selected.

- **Block**

  In this mode, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Windows event log and Kaspersky Security Center event log.

Managing Execution prevention

You can configure component settings either in the Kaspersky Security Center Web Console or locally via the command line.

How to prevent object execution in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Telemetry collection servers → Endpoint Detection and Response (Industrial CyberSecurity)** and click **Configure**.

5. Select the **Enable Execution prevention** check box.

6. In the **Action on execution or opening of forbidden object** block, select the component operating mode:

   - **Block**. In this mode, the application blocks the execution of objects or opening of documents that match prevention rule criteria. The application also publishes an event about attempts to execute objects or open documents to the Windows event log and Kaspersky Security Center event log.

   - **Inform**. In this mode, Kaspersky Industrial CyberSecurity for Nodes publishes an event about attempts to run executable objects or open documents that match prevention rule criteria to the Windows event log and Kaspersky Security Center, but does not block the attempt to run or open the object or document. By default, the mode is selected.

7. Create a list of execution prevention rules:

   a. Click **Add**.

   b. This opens a window; in this window, enter the name of the execution prevention rule.

   c. In the **Type** drop-down list, select the object that you want to block: **Executable file**, **Script**, **Microsoft Office document**.

   If you select a wrong object type, Kaspersky Industrial CyberSecurity for Nodes does not block the file or script.

   d. To add the file, you must enter the hash of the file (SHA256 or MD5), the full path to the file, or both the hash and the path.

   > If the file is located on a network drive, enter the file path starting with `\\`, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, Kaspersky Industrial CyberSecurity for Nodes does not block the file or script.

   e. Click **OK**.

8. Save your changes.

As a result, Kaspersky Industrial CyberSecurity for Nodes blocks the execution of objects: running executable files and scripts, opening office format files. You can, however, for example, open a script file in a text editor even if running the script is prevented. When blocking the execution of an object, Kaspersky Industrial CyberSecurity for Nodes displays a standard notification if notifications are enabled in application settings.

For more details on configuring Execution prevention in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Process start

You can remotely run files using the *Start process* task. For example, you can remotely run an utility that creates the computer configuration file. Next you can use the *Get file* task to receive the created file in Kaspersky Security Center Web Console.

To create a Start process task:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
   The list of tasks opens.
2. Click **Add**.
3. Configure the task settings:
   a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.
   b. In the **Task type** drop-down list, select **Start process**.
   c. In the **Task name** field, enter a brief description of the task and click **Next**.
4. In the **Task scope** section, select managed devices and click **Next**.
5. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.
   By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).
6. Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.
7. Click the new task. The task properties window opens.
8. Select the **Application settings** tab.
9. Select the **Start settings** section and enter the process start command:
   Suppose you want to run an utility (`utility.exe`) that saves the information about the computer's configuration to a file named `conf.txt` in the current folder (by default). The utility is in the `C:\Users\admin\Diagnostic\` folder. You must save the configuration file in the `C:\Users\admin\Documents\Configuration` folder. Enter the following values:
   - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
   - **Command line arguments (optional)** – `/R conf.txt`
   - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`
10. In the task properties window, select the **Schedule** tab.
11. Configure the task schedule.

    Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

12. Click **Save**.
13. Select the check box next to the task and click the **Start** button.

As a result, Kaspersky Industrial CyberSecurity for Nodes runs the command in silent mode and starts the process. You can view the results of the task in task properties in the **Execution results** section.

For more details on running the *Start process* task in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Terminate process

You can remotely terminate processes using the *Terminate process* task. For example, you can remotely terminate an Internet speed testing utility that was started using the *Run process* task.

If you want to prohibit running a file, you can configure Execution prevention. You can prohibit the execution of executable files, scripts, office format files.

> Processes of System Critical Objects (SCO) cannot be terminated. SCOs are files that the operating system and the Kaspersky Industrial CyberSecurity for Nodes application require to be able to run.

To create a Terminate process task:

1. In the main window of the Web Console, select **Devices** → **Tasks**.
   The list of tasks opens.
2. Click **Add**.
3. Configure the task settings:
   a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.
   b. In the **Task type** drop-down list, select **Terminate process**.
   c. In the **Task name** field, enter a brief description of the task and click **Next**.
4. In the **Task scope** section, select managed devices and click **Next**.
5. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.
   By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).
6. Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.
7. Click the new task. The task properties window opens.
8. Select the **Application settings** tab.
9. To complete the process, you must select the file that you want to terminate. You can select a file in one of the following ways:
   - Enter the full name to the file.
   - Enter the hash of the file and the path to the file.
   - Enter the PID of the process (only for local tasks).

If the file is located on a network drive, enter the file path starting with `\\`, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, you can get a *File not found* error.

10. In the task properties window, select the **Schedule** tab.
11. Configure the task schedule.

    Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

12. Click **Save**.
13. Select the check box next to the task and click the **Start** button.

    As a result, Kaspersky Industrial CyberSecurity for Nodes terminates the process on the computer. For example, if a 'GAME' application is running and you terminate the game.exe process, the application is closed without saving data. You can view the results of the task in task properties in the **Results** section.

For more details on running the *Terminate process* task in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Get file

You can get files from user computers. For example, you can configure getting an event log file created by a third-party application. To get the file, you must create a dedicated task. As a result of the execution of the task, the file is saved in Quarantine. You can download this file from Quarantine to your computer using Web Console. On the user's computer, the file remains in its original folder.

For the task to complete successfully, the size of the resulting file must be less than 2 GB.

To create the Get file task:

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

   The list of tasks opens.

2. Click **Add**.
3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.

   b. In the **Task type** drop-down list, select **Get file**.

   c. In the **Task name** field, enter a brief description of the task and click **Next**.

4. In the **Task scope** section, select managed devices and click **Next**.

5. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.

   By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).

6. Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.

7. Click the new task. The task properties window opens.

8. Select the **Application settings** tab.

9. In the list of files, click **Add**. The file adding wizard starts.

10. To add the file, you must enter the full path to the file, or checksum with a folder path.

    > If the file is located on a network drive, enter the file path starting with `\\`, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, you can get a *File not found* error.

11. In the task properties window, select the **Schedule** tab. Configure the task schedule.

    > Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

12. Click **Save**.

13. Select the check box next to the task and click the **Start** button.

As a result, Kaspersky Industrial CyberSecurity for Nodes creates a copy of the file and moves that copy to Quarantine.

To receive a copy of a file in Kaspersky Endpoint Agent, create the **Quarantine file** task and specify that the file does not need to be deleted when it is moved to quarantine in the **Actions after quarantining a file** section. For more details, see the Kaspersky Endpoint Agent Help (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0).

To receive a copy of a file in Kaspersky Industrial CyberSecurity for Linux Nodes, create a task with the **Receiving a file from a device** type. For more details, please refer to the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

> If you are using Kaspersky Endpoint Security 12.1 for Linux, the task is moved to the Backup folder of Kaspersky Security Center.

Delete file

When Kaspersky Industrial CyberSecurity for Nodes is integrated with Kaspersky Industrial CyberSecurity Endpoint Detection and Response, you can delete files from a protected device using the Delete file task.

> System Critical Objects (SCO) cannot be deleted. SCOs are files that the operating system and the Kaspersky Industrial CyberSecurity for Nodes application require to be able to run.

To create the Delete file task:

1. In the main window of the Web Console, select **Asset management** → **Tasks**.
   The list of tasks opens.
2. Click **Add**.
3. Configure the task settings:
   a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.
   b. In the **Task type** drop-down list, select **Delete file**.
   c. In the **Task name** field, enter a brief description of the task and click **Next**.
4. In the **Task scope** section, select managed devices and click **Next**.
5. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.
   By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).
6. Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.
7. Click the new task. The task properties window opens.
8. Select the **Application settings** tab.
9. To delete the file, you must enter the full path to the file, or checksum with a folder path.

   If the file is located on a network drive, enter the file path starting with \\, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, you can get a *File not found* error.

10. In the task properties window, select the **Schedule** tab. Configure the task schedule.

    Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

11. Click **Save**.
12. Select the check box next to the task and click the **Start** button.

As a result, Kaspersky Industrial CyberSecurity for Nodes deletes the file from the computer. If the file is locked by a different process, the task is displayed as *Done*, but the file itself is deleted only after the computer is restarted. After restarting the computer, confirm that the file is deleted.

The *Delete file* task can finish with the *Access denied* error if you are trying to delete an executable file that is currently running. Create a terminate process task for the file and try again.

For more details on deleting files in Kaspersky Endpoint Agent (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and Kaspersky Industrial CyberSecurity for Linux Nodes, see the Kaspersky Endpoint Agent Help (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0) and the Kaspersky Industrial CyberSecurity for Linux Nodes Help.

Move file to Quarantine

One of the possible response actions when a threat is detected is to quarantine the file.

Quarantine is a special local repository on a device with Kaspersky Industrial CyberSecurity Endpoint Detection and Response which is intended for storing files that are probably infected by viruses or cannot be disinfected at the time when they are detected. You can configure Quarantine settings. Quarantined files are stored on the protected device in an encrypted form and therefore do not compromise the device security.

You can quarantine a file manually or configure automatic quarantining of a file as a result of alert response actions. You can also quarantine file from the alert details window.

This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

The extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response allows you to send a quarantined file for analysis to Kaspersky TIP. To use this functionality, you must configure integration with Kaspersky TIP. See Kaspersky Security Center Help for more details.

The Kaspersky Security for Business Professional license includes a limited number of requests to Kaspersky TIP.

For details on managing Quarantine, please refer to the Kaspersky application Help:

- Kaspersky Security Center Help
- Kaspersky Endpoint Agent Help (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0).
- Kaspersky Industrial CyberSecurity for Linux Nodes Help

Viewing quarantined files

To view the list of quarantined files:

In the main window of the Web Console, select **Operations** → **Repositories** → **Quarantine**.

Scanning of objects quarantined by Kaspersky Industrial CyberSecurity Endpoint Detection and Response is not available.

The objects are quarantined with the permissions of the system account. When using Kaspersky Endpoint Agent, files restored from quarantine are not placed in their original location but in a special folder on the device, from which you can manually move them to their destination folder.

Sending a file from Quarantine to Kaspersky TIP

The Kaspersky Security for Business Professional license includes a limited number of requests to Kaspersky TIP.

To send a file from Quarantine to Kaspersky TIP:

1. In the main window of the Web Console, select **Operations** → **Repositories** → **Quarantine**.
2. Select the file.

   You can send only one file at a time for analysis.
3. On the toolbar, click the **Send for threat analysis** button.

   Kaspersky Security Center sends the file from the managed device to Kaspersky TIP. To do this, the managed device must be visible on the network.

The file is sent to Kaspersky TIP. To view the analysis results, click the **View in Kaspersky TIP** button in the notification, and then log in to Kaspersky TIP.

Kaspersky Security Center does not save the Kaspersky TIP analysis results.

Cloud Sandbox

Cloud Sandbox is a cloud-based technology that detects complex threats on user computers. Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Linux Nodes automatically send files requiring verification to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to identify malicious activity and decides on their reputation. Data on these files is then sent to Kaspersky Security Network.

For Cloud Sandbox to operate, you must enable the use of Kaspersky Security Network.

If you are using Kaspersky Private Security Network, Cloud Sandbox technology is not available.

To use Cloud Sandbox technology on devices running Linux, the following conditions must be met:

- Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 or later must be installed on the computer.
- KSN support is included in Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0 or later.

For more information about Cloud Sandbox support, see the *Kaspersky Industrial CyberSecurity for Linux Nodes Help*.

In Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0 or later, you can enable a separate counter for threats detected by Cloud Sandbox. You can use this counter to generate statistics during analysis of detected threats.

To view reports on alerts detected by Cloud Sandbox (**Report on threats** → the **Details** tab → the **Detected by Cloud Sandbox technology** column), you must have Kaspersky Security Center for Windows version 14.2 or later, Kaspersky Security Center for Linux version 15.1 or later, or Kaspersky Security Center Cloud Console.

Working with alert details

This section contains information about actions that can be performed directly from the alert details window.

About alert details

Alert details contain all available information about the detected threat and allow you to manage alert response actions.

Alert details contain the following information:

- **Threat development chain graph**. Displays the attack lifecycle targeting the endpoint device. The alert details card displays two versions of the graph: a condensed version and a complete version.
  - The condensed version contains the following key elements:
    - **Asset** is the device on which the alert was detected.
    - **User** is the user associated with the alert.
    - **Root cause** is the root cause of the event.
    - **Detected object** is the threat name.
    - **Decision** is the decision made by the EPP program regarding the threat.
    - Result of performing the action
  - A complete graph contains the entire chain of events related to an attack, shows the path of attack escalation, the processes involved in the attack, and the actions performed by those processes.
- **Recommendations**. Recommendations for responding to an alert.

  Recommendations are available in Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 and later.
- **Alert details**. General information about the alert, including the processing result, category, and detection mode (for example, detection during on-demand scan or during automatic scan).
- **Device**. Information about the protected device on which the alert occurred. For example, the device name, IP address, MAC address, and operating system.
- **Process**. Information about the process that was classified as malicious.
- **File**. Information about detected object.

- **Download**. Information about the process that accessed the network resource and triggered the alert.
- **Data from Kaspersky TIP**. Information about file reputation, including its trust group, digital signature, file distribution data, and a link to alert analytics.

  This information is available if the Kaspersky Security Network function is enabled in the Kaspersky Industrial CyberSecurity for Linux Nodes application at the time of detection.

  > The listed data is specified at the time of detection of the threat. The solution does not update the listed data; therefore, it may differ from the data displayed on the Kaspersky Threat Intelligence Portal. To view the latest data, use the links to the Kaspersky Threat Intelligence Portal data in the alert details.

Additional information about the response actions taken on objects in the threat development chain is provided if both of the following applications are used alongside Kaspersky Security Center:

- Kaspersky Industrial CyberSecurity for Nodes 4.5 and later.
- Endpoint Detection and Response web plug-in version 15.4 or later.

You can perform the following response actions from the alert details:

- Isolate the device on which the alert occurred.
- Quarantine file.

  > This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

- Create an IOC Scan task.
- Prevent execution of a detected file.

  > This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

EPP applications generate alerts based on threat detection events and the results of threat data processing. The event storage interval can be configured in the EPP application.

> By default, the EPP application stores alert details for 30 days. After this period, alert details are automatically deleted.

The **Alerts** list displays alerts for the last 30 days.

Viewing alert details

Alert details are available in the list of alerts. The list of alerts is available in the **Report on threats** or in the **Alerts** subsection of the **Monitoring** section in Kaspersky Security Center Web Console.

If you add a license key for Kaspersky Industrial CyberSecurity Endpoint Detection and Response, the **Alerts** subsection will automatically appear in the main menu in the **Monitoring** section. You can also configure the displaying of the **Alerts** subsection in the properties of Kaspersky Security Center.

To view alert details:

1. In the main Kaspersky Security Center Web Console window, go to the **Monitoring** → **Alerts** section.

   With the extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response, you can group similar alerts using the **Alerts aggregation** toggle switch.

2. Select the alert and click the **Enriched** link.

   The alert details are displayed.

To view the alert details in the report on threats:

1. In the main Kaspersky Security Center Web Console window, go to the **Monitoring** → **Reports** section.
2. Select the **Report on threats** template and click the **Show report** button.
3. In the report window, on the **Details** tab, select the alert and click the **Open alert details** link.

   The alert details are displayed.

To display the alert details, Kaspersky Industrial CyberSecurity Endpoint Detection and Response needs to get data from the device on which the alert occurred. If the data or the device is not available, an error message is displayed. The device response time may take several minutes.

Applying and removing network isolation

To isolate a device from the network from the alert details window:

1. Open the alert details window.
2. Under **Device**, in the **Response actions** drop-down list, select **Isolate device from the network**.

   In Kaspersky Industrial CyberSecurity for Nodes versions 4.5 and later, you can configure network isolation settings for a device.

3. If you want to specify a custom network isolation interval, clear the **Use default unlock settings** check box, and then enter the desired number of hours in the **Unlock after (hours)** field.

4. Click **Isolate**.
5. Confirm the action.

The application will isolate the device and assign it the ISOLATED FROM NETWORK tag.

To remove network isolation from a device:

1. Open the alert details window.
2. Under **Device**, in the **Response actions** drop-down list, select **Re-enable device on the network**.

   The **Re-enable device on the network** button is available if the alert was received from Kaspersky Industrial CyberSecurity for Nodes version 4.5 or later or Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 or later.

3. Confirm the action.

The device network isolation will be removed, and the ISOLATED FROM NETWORK tag assigned to the device will be deleted.

For more details on enabling and disabling network isolation on a device and configuring network isolation exclusions, see the following sections:

- Kaspersky Endpoint Agent Help (when using Kaspersky Industrial CyberSecurity for Nodes versions 3.1 to 4.0).
- Kaspersky Industrial CyberSecurity for Linux Nodes Help

Moving a file to Quarantine from alert details

To move a file to Quarantine from the alert details:

1. Open the alert details.
2. Under **File**, in the **Response actions** drop-down list, click the **Move to quarantine** button.

   The file will be deleted from the device, and its copy will be quarantined.

This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

Creating IOC Scan task from alert details

To create an IOC Scan task from the alert details:

1. Open the alert details.
2. On the **All alert events** tab, select the items from which you want to create an IOC Scan task.

3. Click **Create IOC**.

4. Select the triggering criteria for the compromise indicator:

   - If you want the indicator of compromise to be triggered when any of the selected objects is detected, select **OR (any IOC found)** on the right side of the screen.

   - If you want the indicator of compromise to be triggered when all the selected objects are detected, select **AND (all IOC found)** on the right side of the screen.

5. Select the actions to be taken when the IOC is triggered:

   - Isolate device from the network.

   - Start critical areas scan.

   - Quarantine a copy, delete the object.

6. Click **Create task**.

   You can view the created tasks in the **Devices** → **Tasks** section.

   When you create an IOC Scan task for the selected object (file or process) from the alert details, an IOC with the FileItem term is automatically created.

Preventing object execution from the alert details

Execution prevention rules are applied to the device on which the alert occurred if an active policy for Kaspersky Industrial CyberSecurity for Nodes is applied to this device. If the device, on which the alert occurred, is not managed by an active policy, the Execution prevention rule will not be created.

To prevent object execution from the alert details:

1. Open the alert details.

2. In the **File** section click the **Prevent execution** button.

   Object execution will be prevented. Execution prevention rule will be added to the policy for the group the device belongs to.

This action is not available on computers running Linux operating systems with Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 installed.

Response actions for Active Directory users from alert details

The extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response allows you to perform response actions for Active Directory users affected by or involved in the alert. You can perform the following response actions:

- Resetting the user password.
- Blocking a user account.
- Adding a user to a security group.
- Removing a user from a security group.

> These response actions are available only on protected devices with Kaspersky Industrial CyberSecurity for Nodes 4.5 and later installed.

To use this functionality, you must configure integration with Active Directory. See Kaspersky Security Center Help for more details.

Resetting the user password

> For a user whose Active Directory account properties have the **User cannot change password** setting enabled, the **Reset password** response action will not be executed.

To reset an Active Directory user password from the alert details:

1. Open the alert details.
2. Go to **Alert Details** → the **File** settings group, and then in the **Owner** field, select **Reset password** from the drop-down list.

   The Active Directory user password will be reset.

If the **Password never expires** setting is enabled in the Active Directory user account properties, after the **Reset password** response action is executed, the **Password never expires** setting will be disabled, and the user will be required to change their domain password the next time they log in.

Blocking a user account

To block an Active Directory user account from alert details:

1. Open the alert details.
2. Go to **Alert Details** → the **File** settings group, and then in the **Owner** field, select **Block user account** from the drop-down list.

The Active Directory user account will be blocked.

Adding a user to a security group

To add an Active Directory user to a security group from the alert details:

1. Open the alert details.
2. Go to **Alert Details** → the **File** settings group, and then in the **Owner** field, select **Add user to security group** from the drop-down list.

   The **Add user to security group** window opens.
3. Enter the full path to the security group.
4. Click the **Add** button.

The user will be added to the security group. It may take up to 12 hours for the user security group information to be updated.

Removing a user from a security group

To remove an Active Directory user from a security group from the alert details:

1. Open the alert details.
2. Go to **Alert Details** → the **File** settings group, and then in the **Owner** field, select **Remove user from security group** from the drop-down list.

   This opens a **Remove user from security group** window.
3. Enter the full path to the security group.
4. Click the **Delete** button.

The user will be removed from the security group. It may take up to 12 hours for the user security group information to be updated.

Assigning Kaspersky ASAP training courses to users from alert details

The extended functionality of Kaspersky Industrial CyberSecurity Endpoint Detection and Response allows you to assign Kaspersky Automated Security Awareness Platform training courses to users who work with alerts, directly from the alert details.

To use this functionality, you must configure integration with Active Directory and Kaspersky ASAP. For more information, see the following Kaspersky Security Center Help articles: Configuring integration with Active Directory, Configuring integration with Kaspersky Automated Security Awareness Platform.

To assign Kaspersky ASAP training courses from the alert details:

1. Open the alert details.
2. Go to **Alert Details** → the **File** settings group, and then in the **Owner** field, select **Assign KASAP course** from the drop-down list.

   The **User details** window opens.
3. In the **Assign KASAP group** drop-down list, select a training group for the user.

The selected group will be assigned to the user.

You can view the assigned training course in the **User details** window, in the **Assigned courses** section.

Monitoring & Reporting

The following features are available to monitor operation of Kaspersky Industrial CyberSecurity Endpoint Detection and Response:

- EDR alerts widget
- List of alerts
- Kaspersky Security Center reports and selections

Viewing the list of alerts

To view all alerts as a list,

In the Web Console, select **Monitoring** → **Alerts**.

The **Alerts** section is displayed automatically after Kaspersky Industrial CyberSecurity Endpoint Detection and Response activation. You can also enable display of this section in Kaspersky Security Center.

From the list of alerts, you can open the details of the selected alert.

Viewing information about triggering of the Execution prevention rules

Kaspersky Security Center functionality allows you to get information about the applications, execution of which was prevented by Kaspersky Industrial CyberSecurity Endpoint Detection and Response as a result of the triggering the execution prevention rules.

To view a report on the applications prevented from execution:

1. In the Web Console, select **Monitoring** → **Reports**.
2. Select the required report from the list:
   - **Report on prohibited applications** – to view information about the applications that were prevented from execution in the Block and log to the report mode.
   - **Report on prohibited applications in test mode** – to view information about the applications that were prevented from execution in the Log events only mode.

Viewing a list of isolated devices

Kaspersky Security Center functionality allows you to get information about the devices with enabled network isolation.

You can get this information by generating a selection of devices using the ISOLATED FROM NETWORK tag.

> In Kaspersky Security Center Web Console, you can generate a selection of isolated devices on a physical Administration Server only after network isolation was applied at least once on this server.

To view a list of devices isolated from the network:

1. Go to **Asset management** → **Tags** → **Device tags**.
2. In the ISOLATED FROM NETWORK tag field, click the **View devices** button.

   This opens the list of isolated devices.

To generate a selection of devices isolated from the network:

1. In Kaspersky Security Center Web Console, go to the **Asset management** → **Device selections** section.
2. Click the **Add** button to create a device selection.
3. Create a new condition and select the **Tags** tab.
4. Click **Add**.
5. In the **Add tag** window, select **All devices that have this tag**, and in the **Tag** drop-down list, select ISOLATED FROM NETWORK.

6. Click **Save** in all open windows.

7. Confirm opening the created selection.

The new selection displays a list of devices isolated from the network.

Endpoint Agent mode

Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode allows deploying Kaspersky Detection and Response solutions from alongside third-party EPP applications. The Endpoint Agent configuration is installed on individual workstations and servers of the organization's IT infrastructure and continuously monitors processes running on computers, open network connections, and files being modified. In this mode, the protection and control components of Kaspersky Industrial CyberSecurity for Nodes are not available.

Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode supports the following Kaspersky solutions:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response Expert (on-premise)

In addition, the Endpoint Agent mode includes integration with the Kaspersky Industrial CyberSecurity for Networks application and the Anomaly Detection using Sigma rules functionality.

Installing Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode

The installation process of Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode is the same as installing Kaspersky Industrial CyberSecurity for Nodes; in the installation package settings or the Setup Wizard, at the application component selection step, select Endpoint Agent.

After installing Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode, the Application Console becomes available, as well as the application icon in the system tray .

In Kaspersky Security Center Administration Console, the computer with the installed application in Endpoint Agent mode has the *Critical* status: . The computer has this status because the Real-Time File Protection component is missing. You do not need to take any action.

If you could not install Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode on a computer with a third-party EPP application because the installer found incompatible software on the computer, you can disable the incompatible software check when installing the application.

Compatibility with third-party EPP applications

Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode is compatible with EPP applications of the following vendors:

- **Bitdefender**

  Bitdefender Endpoint Security Tools version 8.26.7.647.

- **Dallas Lock**

  Dallas Lock 8.0-C version 843.2.

- **ESET**

  ESET Endpoint Security version 13.0.2044.0 and ESET Management Agent version 13.2.1189.0.

- **Secret Net Studio**

  Secret Net Studio version 8.11 (20851).

  > The application cannot be installed on a computer where Secret Net Studio is deployed with the Antivirus component. To make interoperability possible, you must remove the Antivirus component from Secret Net Studio.

- **Sophos**

  Sophos Intercept X version 2024.1.2 or later (including Endpoint Agent and Sophos Core Agent version 2026.2.1.3).

- **Trend Micro**

  Trend Micro Vision One Apex One (including Security Agent 14.0.20731).

  Trend Micro Deep Security version 20.0.3-18160 (including Security Agent).

- **Microsoft**

  Microsoft Defender Antivirus, part of Windows Security (formerly Windows Defender).

The applications must be installed in the following order: first, install the EPP application, then Kaspersky Security Center Network Agent, then Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode. This is necessary because the installer of the EPP application may detect Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode and the Network Agent as incompatible software and remove them. The operation of the application in Endpoint Agent mode and the Network Agent should also be checked after updating the third-party EPP application because its installer may re-scan the computer for incompatible software and remove the applications.

Managed Detection and Response

Kaspersky Industrial CyberSecurity for Nodes supports integration with the Managed Detection and Response solution.

Kaspersky Managed Detection and Response (also referred to as MDR) delivers round-the-clock protection from the growing volume of threats that circumvent automated security barriers to organizations who struggle to find the expertise and staff or possess limited in-house resources. Unlike similar offerings on the market, this service leverages a proven track record of effective targeted attack research to ensure continuous defense against even the most complex threats. The service helps improve your corporate resilience to cyberthreats, while freeing up your existing resources to focus their attention on other tasks.

MDR uses telemetry data received from endpoints and machine learning. MDR sends incident data to Kaspersky experts. The experts can then process the incident and, for example, add a new entry to Anti-Virus databases. Alternatively, the experts can issue recommendations on processing the incident and, for example, suggest isolating computer from the network. For detailed information about how the solution works, please refer to the Kaspersky Managed Detection and Response Help.

Configurations of Kaspersky Industrial CyberSecurity for Nodes for integrating with MDR

The following configurations can be used to work with MDR:

- **[KICS+built-in agent]**. In this configuration, Kaspersky Industrial CyberSecurity for Nodes acts as both the application that ensures the security of the computer and the application for working with MDR. The built-in agent is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.

- **[Third-party EPP+KICS in Endpoint Agent mode]**. In this configuration, the security of the IT infrastructure is provided by the third-party Endpoint Protection Platform (EPP). Integration with MDR is provided by Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode. The Endpoint Agent mode is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.

Configuring MDR integration

Integration with Kaspersky Managed Detection and Response consists of the following steps:

1. **Installing the Managed Detection and Response (Industrial CyberSecurity) component**

   For integration of Kaspersky Industrial CyberSecurity for Nodes with the Managed Detection and Response solution, the Managed Detection and Response (Industrial CyberSecurity) component is used. To install this component using the installation package settings or the Setup Wizard, or when changing the configuration of the application components in the Windows Control Panel, select:

   - **Full functionality → Endpoint Agent → Managed Detection and Response (Industrial CyberSecurity)** for the built-in agent

   - **Endpoint Agent → Managed Detection and Response (Industrial CyberSecurity)** for the Endpoint Agent configuration

   You can also install the component using the *Change Kaspersky Industrial CyberSecurity for Nodes components* task.

   > To install the Managed Detection and Response (Industrial CyberSecurity) component without restarting the computer using the *Change Kaspersky Industrial CyberSecurity for Nodes components* task, you need to disable the **Check for incompatible third-party applications** option in the task settings.

2. **Configuring Kaspersky Private Security Network**

Starting with the July 2025 update, the Managed Detection and Response solution supports operation without the KPSN configuration file. For detailed information on how the MDR solution uses Kaspersky Security Network, refer to the Kaspersky Managed Detection and Response Help.

If your configuration does not meet the requirements for running without KPSN configuration files, upload the KPSN configuration file in the Administration Server properties. The KPSN configuration file is located inside the ZIP archive of the MDR configuration file. You can also upload the KPSN configuration file using the command line.

For details on configuring Kaspersky Private Security Network, please refer to the Kaspersky Security Center Help.

3 **Activating Kaspersky Managed Detection and Response**

When upgrading Kaspersky Industrial CyberSecurity for Nodes from an earlier version to version 4.5 or later, the Managed Detection and Response solution that was previously activated using an MDR configuration file (BLOB file) will not be activated automatically. You need to reactivate the Managed Detection and Response solution using a key file or an activation code.

To activate the Managed Detection and Response solution in Kaspersky Industrial CyberSecurity for Nodes, you need a separate license for Kaspersky Managed Detection and Response for Industrial CyberSecurity Add-on.

Starting with version 4.5, Kaspersky Industrial CyberSecurity for Nodes does not support activating the Managed Detection and Response solution using only the MDR configuration file (BLOB file).

If you are using MDR tenants, you need to upload the BLOB file for the tenant before applying the activation code, even if the BLOB file has expired.

If you do not use and have never created MDR tenants, you do not need to upload the BLOB file.

For detailed information on activating the solution, refer to the Kaspersky Managed Detection and Response Help.

4 **Enabling the Managed Detection and Response (Industrial CyberSecurity) component**

How to enable the Managed Detection and Response (Industrial CyberSecurity) component in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Telemetry collection servers** section.
4. In the **Managed Detection and Response (Industrial CyberSecurity)** block, click the **Settings** button.

   The **Managed Detection and Response (Industrial CyberSecurity)** window opens.
5. Select the **Managed Detection and Response** check box.

6. If necessary, upload the MDR configuration file by clicking the **Upload** button. For detailed information about the MDR configuration file, please refer to the Kaspersky Managed Detection and Response Help.

   By uploading a Managed Detection and Response configuration file, you agree to automatically transmit the specified data from the device with pre-installed Kaspersky Industrial CyberSecurity for Nodes to Kaspersky for processing. Do not upload the configuration file if you do not want the specified information to be processed.

7. Save your changes.

How to enable the Managed Detection and Response (Industrial CyberSecurity) component in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Managed Detection and Response (Industrial CyberSecurity)** block, click the **Settings** button.

   The **Managed Detection and Response (Industrial CyberSecurity)** window opens.

6. Select the **Managed Detection and Response (Industrial CyberSecurity) DISABLED** check box.
7. If necessary, upload the MDR configuration file by clicking the **Upload** button. For detailed information about the MDR configuration file, please refer to the Kaspersky Managed Detection and Response Help.

   By uploading a Managed Detection and Response configuration file, you agree to automatically transmit the specified data from the device with pre-installed Kaspersky Industrial CyberSecurity for Nodes to Kaspersky for processing. Do not upload the configuration file if you do not want the specified information to be processed.

8. Save your changes.

How to enable the Managed Detection and Response (Industrial CyberSecurity) component in the Application Console

1. In the Application Console tree, select the **Telemetry collection servers** → **Managed Detection and Response (Industrial CyberSecurity)** section.
2. Click the **Properties** link in the results pane.

   The **Managed Detection and Response (Industrial CyberSecurity)** window opens on the **General** tab.

3. Select the **Managed Detection and Response** check box.

4. If necessary, upload the MDR configuration file by clicking the **Upload** button. For detailed information about the MDR configuration file, please refer to the Kaspersky Managed Detection and Response Help.

   By uploading a Managed Detection and Response configuration file, you agree to automatically transmit the specified data from the device with pre-installed Kaspersky Industrial CyberSecurity for Nodes to Kaspersky for processing. Do not upload the configuration file if you do not want the specified information to be processed.

5. Save your changes.

You can also enable the Managed Detection and Response (Industrial CyberSecurity) component using the command line.

5. **Configuring other components of the application to receive telemetry**

   You must enable the following components for Kaspersky Managed Detection and Response to work:

   - Kaspersky Security Network (extended mode).
   - Real-Time File Protection.
   - AMSI Scanner.
   - Anti-Cryptor
   - Exploit Prevention.
   - Network Threat Protection.
   - Firewall.
   - On-Demand Scan.

   For Kaspersky Managed Detection and Response to work with Administration Server via Kaspersky Security Center Web Console, you must also establish a new secure connection, a *background connection*. Kaspersky Managed Detection and Response prompts you to establish a background connection when you deploy the solution. Make sure the background connection is established.

   Establishing a background connection in Kaspersky Security Center Web Console

   1. In the main window of the Web Console, select **Settings** → **Integration**.
   2. Go to the **Integration** section.
   3. Turn on the **Background connection for integration Enabled** toggle.
   4. Save your changes.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform is a solution for protection of an organization's IT infrastructure and early detection of threats such as zero-day attacks, targeted attacks, and advanced persistent threats (hereinafter also referred to as APT).

Kaspersky Anti Targeted Attack Platform solution includes three functional units:

- Kaspersky Anti Targeted Attack (hereinafter also referred to as KATA) – protects the enterprise's IT infrastructure perimeter.
- Kaspersky Endpoint Detection and Response (hereinafter also KEDR) – protects computers in the organization local network.
- Network Detection and Response, which protects the corporate LAN.

For details about the solution, please refer to the Kaspersky Anti Targeted Attack Platform Help.

Principle of operation of the solution

Kaspersky Industrial CyberSecurity for Nodes is installed on individual computers running Windows that are included in the organization's IT infrastructure. The application constantly monitors processes, open network connections, and files being modified. Information about events on the computer, threats detected by the application, and the results of processing these threats is sent to the Central Node server.

Integration with KEDR (KATA) is configured in the Kaspersky Security Center Administration Console or Kaspersky Security Center Web Console. The built-in agent or the application in Endpoint Agent mode is then managed using the Kaspersky Anti Targeted Attack Platform console, including running tasks, managing quarantined objects, viewing reports, and other actions.

Kaspersky Industrial CyberSecurity for Nodes configurations for integration with Kaspersky Anti Targeted Attack Platform

Kaspersky Industrial CyberSecurity for Nodes can be integrated with Kaspersky Endpoint Detection and Response as part of the Kaspersky Anti Targeted Attack Platform solution. The following configurations are possible:

- **[KICS+built-in agent]**. In this configuration, Kaspersky Industrial CyberSecurity for Nodes acts as both the application that ensures the security of the computer and the application for working with KEDR. The built-in agent is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.
- **[Third-party EPP+KICS in Endpoint Agent mode]**. In this configuration, the security of the IT infrastructure is provided by the third-party Endpoint Protection Platform (EPP). Integration with KEDR is provided by Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode. The Endpoint Agent mode is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.

Support for previous versions of Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes 4.5 supports integration with the Kaspersky Anti Targeted Attack Platform (EDR) solution using the built-in agent or the Endpoint Agent mode; you do not need to install Kaspersky Endpoint Agent.

If you are using Kaspersky Industrial CyberSecurity for Nodes older than 4.5 for integration with Kaspersky Anti Targeted Attack Platform (EDR), you must install Kaspersky Endpoint Agent separately.

Configuring KATA integration

Starting with Kaspersky Industrial CyberSecurity for Nodes 4.5, the KATA Integration component has been renamed to Endpoint Detection and Response Expert (on-premises). In this version of the application, the component is compatible with Kaspersky Anti Targeted Attack Platform 7.1 and earlier versions, as well as Kaspersky Endpoint Detection and Response Expert (on-premises).

The Endpoint Detection and Response (Industrial CyberSecurity) and Endpoint Detection and Response Expert (on-premises) components are not compatible with each other.

The following conditions must be satisfied for integration of the Kaspersky Industrial CyberSecurity for Nodes built-in agent with KATA:

- Kaspersky Anti Targeted Attack Platform 5.0 or later must be deployed in the corporate IT infrastructure.
- Kaspersky Security Center 14.2 or later must be deployed in the corporate IT infrastructure.
- Application components that send data to KATA must be enabled and functioning:
  - Real-Time File Protection
  - Exploit Prevention
  - Anti-Cryptor
  - AMSI Scanner
  - Kaspersky Security Network

To integrate the Endpoint Agent configuration with KATA in the corporate IT infrastructure, the following must be deployed:

- Kaspersky Anti Targeted Attack Platform version 5.0 or higher.
- Kaspersky Security Center version 14.2 or higher.

Setting up KATA Integration involves the following steps:

1. **Installing the Endpoint Detection and Response Expert (on-premises) component**

   In installation package settings or in the Setup Wizard, or by changing the set of application components in the Windows Control Panel, at the step when you must select application components for installation, select the following:

   - **Full functionality → Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** for the built-in agent
   - **Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** for the Endpoint Agent configuration

To finish changing the set of application components, you must restart the computer.

2. **Endpoint Detection and Response Expert (on-premises) activation**

You need to purchase a separate license for KATA (for example, Kaspersky Endpoint Detection and Response (KATA) Add-on).

Licensing of the stand-alone Endpoint Detection and Response Expert (on-premises) functionality is the same as the licensing of Kaspersky Industrial CyberSecurity for Nodes. The feature becomes available after you add a separate key for Kaspersky Endpoint Detection and Response (KATA). As a result, two keys will be added on the computer: a key for Kaspersky Industrial CyberSecurity for Nodes and a key for Endpoint Detection and Response Expert (on-premises).

Make sure that the Endpoint Detection and Response Expert (on-premises) functionality is included in the license.

3. **Connecting to Central Node**

For Kaspersky Anti Targeted Attack Platform, you can establish a trusted connection between Kaspersky Industrial CyberSecurity for Nodes and the Central Node component. To configure a trusted connection, you must use a TLS certificate. You can get a TLS certificate in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help). Then you must add the TLS certificate to Kaspersky Industrial CyberSecurity for Nodes (see instructions below).

By default, Kaspersky Industrial CyberSecurity for Nodes only checks the TLS certificate of Central Node. To make the connection more secure, you can additionally enable the additional verification of the computer on Central Node. To enable this verification, you must turn on two-way authentication in Central Node and Kaspersky Industrial CyberSecurity for Nodes settings. To use two-way authentication, you will also need a crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help).

How to connect a Kaspersky Industrial CyberSecurity for Nodes computer to Central Node using the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select a policy for managing the application and double-click it to open its settings window.
4. Select the **Telemetry collection servers** section.
5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Settings** button.

   The **Endpoint Detection and Response Expert (on-premises)** window opens.
6. Select the **Endpoint Detection and Response Expert (version 7.1 or earlier)** check box.
7. Under **Connection settings**, click **Add** to add one or more Central Node servers. For each server, specify an address (IPv4, IPv6) and port for connecting to the server.

   Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection with the server at the first IP address. If a connection cannot be established, Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection at the second IP address in the list and so on.
8. Click **Server connection settings**.

9. In the window that opens, configure the connection to the servers:

   - **Timeout (sec)**. Maximum Central Node server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different Central Node server.
   - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Central Node server. You can get a TLS certificate in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help).
   - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Central Node. To use two-way authentication, you need to enable two-way authentication in the Central Node settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help). After configuring the Central Node settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

     The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

10. Click **OK**.
11. If necessary, configure telemetry.
12. Save your changes.

How to connect a Kaspersky Industrial CyberSecurity for Nodes computer to Central Node using the Application Console

1. In the Application Console tree, select the **Telemetry collection servers → Endpoint Detection and Response Expert (on-premises)** section.
2. Click the **Properties** link in the results pane.

   The **Properties: Endpoint Detection and Response Expert (on-premises)** window opens on the **General** tab.
3. Select the **Endpoint Detection and Response Expert (version 7.1 or earlier)** check box.
4. Under **Connection settings**, click **Add** to add one or more Central Node servers. For each server, specify an address (IPv4, IPv6) and port for connecting to the server.

   Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection with the server at the first IP address. If a connection cannot be established, Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection at the second IP address in the list and so on.
5. Click **Server connection settings**.

6. In the window that opens, configure the connection to the servers:

   - **Timeout (sec)**. Maximum Central Node server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different Central Node server.
   - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Central Node server. You can get a TLS certificate in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help).
   - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Central Node. To use two-way authentication, you need to enable two-way authentication in the Central Node settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help). After configuring the Central Node settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

     The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

7. Click **OK**.
8. If necessary, configure telemetry.
9. Save your changes.

How to connect a Kaspersky Industrial CyberSecurity for Nodes computer to Central Node using the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Configure** button.

   The **Endpoint Detection and Response Expert (on-premises)** window opens.
6. Select the **Enable Endpoint Detection and Response Expert (on-premises)** check box.
7. Select the **Endpoint Detection and Response Expert (version 7.1 or earlier)** mode.
8. Under **Connection settings**, click **Add** to add one or more Central Node servers. For each server, specify an address (IPv4, IPv6) and port for connecting to the server.

   Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection with the server at the first IP address. If a connection cannot be established, Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection at the second IP address in the list and so on.
9. Click **Settings for connecting to KATA servers**.

10. In the window that opens, configure the connection to the servers:

    - **Timeout (sec)**. Maximum Central Node server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different Central Node server.
    - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Central Node server. You can get a TLS certificate in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help).
    - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Central Node. To use two-way authentication, you need to enable two-way authentication in the Central Node settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help). After configuring the Central Node settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

      The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

11. Click **OK**.
12. If necessary, configure telemetry.
13. Save your changes.

As a result, the Kaspersky Industrial CyberSecurity for Nodes computer is added using the Kaspersky Anti Targeted Attack Platform console.

Configuring telemetry

Telemetry is a list of events that have occurred on the protected computer. Kaspersky Industrial CyberSecurity for Nodes analyzes telemetry data and sends it to Kaspersky Anti Targeted Attack Platform during synchronization. Telemetry events arrive on the server almost continuously. Kaspersky Industrial CyberSecurity for Nodes initiates synchronization with the server when any of the following conditions are satisfied:

- Synchronization interval has run out.
- The number of events in the buffer exceeds the upper limit.

You can configure the synchronization behavior in the Kaspersky Industrial CyberSecurity for Nodes policy and select optimum values to match your network load.

If there is no connection between Kaspersky Industrial CyberSecurity for Nodes and the server, the application queues new events. When the connection is restored, Kaspersky Industrial CyberSecurity for Nodes sends queued events to the server in proper order. To avoid overloading the server, Kaspersky Industrial CyberSecurity for Nodes may skip some events. To enable this, you can optimize event transmission settings, for example, to set a maximum events-per-hour value.

If you are using Kaspersky Anti Targeted Attack Platform together with another solution which also uses telemetry, you can turn off telemetry for KATA. This lets you optimize server load for these solutions. For example, if you have Managed Detection and Response and Kaspersky Anti Targeted Attack Platform solutions deployed, you can use Managed Detection and Response telemetry while creating threat response tasks in Kaspersky Anti Targeted Attack Platform.

How to configure telemetry in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select a policy for managing the application and double-click it to open its settings window.
4. Select the **Telemetry collection servers** section.
5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Settings** button.
6. In the window that opens, configure the **Send sync request to KATA server every (min)** setting. Frequency of synchronization requests sent to the server. During synchronization, Kaspersky Industrial CyberSecurity for Nodes sends information about modified application settings and tasks.
7. Make sure that the **Send telemetry to KATA** check box is selected in the **Data transmission settings** block.
8. If necessary, configure the **Maximum event transmission delay (sec)** setting: When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.
9. If necessary, configure the **Maximum number of event packages** setting: This setting regulates the maximum number of packets that can be sent as part of one transaction. The default value is 1024.
10. If necessary, select the **Enable request throttling** check box in the **Request throttling** block.

    This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.
11. Configure optimization settings for sending events to the server:

    - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.
    - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.
12. Save your changes.

How to configure telemetry in the Application Console

1. In the Application Console tree, select the **Telemetry collection servers** → **Endpoint Detection and Response Expert (on-premises)** section.

2. Click the **Properties** link in the results pane.

3. In the window that opens, configure the **Send sync request to KATA server every (min)** setting. Frequency of synchronization requests sent to the server. During synchronization, Kaspersky Industrial CyberSecurity for Nodes sends information about modified application settings and tasks.

4. Make sure that the **Send telemetry to KATA** check box is selected in the **Data transmission settings** block.

5. If necessary, configure the **Maximum event transmission delay (sec)** setting: When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.

6. If necessary, configure the **Maximum number of event packages** setting: This setting regulates the maximum number of packets that can be sent as part of one transaction. The default value is 1024.

7. If necessary, select the **Enable request throttling** check box in the **Request throttling** block.

   This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

8. Configure optimization settings for sending events to the server:

   - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

   - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.

9. Save your changes.

How to configure telemetry in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Telemetry collection servers** section.

5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Configure** button.

6. In the window that opens, configure the **Send sync request to server every (min)** setting. Frequency of synchronization requests sent to the server. During synchronization, Kaspersky Industrial CyberSecurity for Nodes sends information about modified application settings and tasks.

7. Make sure that the **Send telemetry to KATA** check box is selected in the **Data transmission settings** block.

8. If necessary, configure the **Maximum event transmission delay (sec)** setting: When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.

9. If necessary, configure the **Maximum number of event packages** setting: This setting regulates the maximum number of packets that can be sent as part of one transaction. The default value is 1024.

10. If necessary, select the **Enable throttling** check box in the **Throttling** block.

    This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

11. Configure optimization settings for sending events to the server:

    - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

    - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.

12. Save your changes.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Industrial CyberSecurity for Nodes supports integration with the Kaspersky Endpoint Detection and Response Expert (on-premises) solution. Kaspersky Endpoint Detection and Response Expert (on-premises) is an enterprise cybersecurity solution that includes Kaspersky applications that allow an organization to defend against most types of cyber risks and cover the most important threat propagation scenarios. EDR Expert (on-premises) components are deployed on the Open Single Management Platform (OSMP). This platform runs cross-platform scenarios in a single interface and allows integrating Kaspersky applications with third-party applications into a comprehensive security system.

One of the central elements of the solution is *SIEM*. SIEM tracks events coming from all components and correlates these events with each other using vendor and user-defined rules. EDR Expert (on-premises) looks at logs and telemetry received from the corporate infrastructure to automatically detect attacks and allows investigating incidents using a unified investigation graph which combines all events collected in EDR Expert (on-premises), including events from Kaspersky applications and third-party information security products.

For response to advanced incidents, EDR Expert (on-premises) uses preset and user-defined scenarios. You can also use response actions from third-party applications and response scenarios that involve multiple applications.

Threat Intelligence tools

Kaspersky Endpoint Detection and Response uses the following Threat Intelligence tools:

- Integration with Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and web addresses.
- Kaspersky Threats database.
- The Kaspersky Security Network cloud service infrastructure, which provides access to real-time file, website, and software reputation information from the Kaspersky knowledge base. Using data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

Principle of operation of the solution

Kaspersky Industrial CyberSecurity for Nodes is installed on individual computers running Windows that are included in the organization's IT infrastructure. The application constantly monitors processes, open network connections, and files being modified. Information about events on the computer, threats detected by the application, and the results of processing these threats is sent to the EDR Expert (on-premises) server.

The EDR Expert (on-premises) integration is configured in the Kaspersky Security Center Web Console. The built-in agent or the application in Endpoint Agent mode is then managed using the Open Single Management Platform (OSMP), including running tasks, managing quarantined objects, viewing reports, and other actions.

Kaspersky Industrial CyberSecurity for Nodes configurations for integration with Kaspersky Anti Targeted Attack Platform

The following configurations can be used for working with EDR Expert (on-premises):

- **[KICS+built-in agent]**. In this configuration, Kaspersky Industrial CyberSecurity for Nodes acts as both the application that ensures the security of the computer and the application for working with EDR Expert (on-premises). The built-in agent supports integration with EDR Expert (on-premises) starting with version 4.5.
- **[Third-party EPP+KICS in Endpoint Agent mode]**. In this configuration, the security of the IT infrastructure is provided by the third-party Endpoint Protection Platform (EPP). Integration with EDR Expert (on-premises) is provided by Kaspersky Industrial CyberSecurity for Nodes in the Endpoint Agent configuration. The Endpoint Agent configuration supports integration with EDR Expert (on-premises) starting with version 4.5.

Configuring EDR Expert (on-premises) integration

The Endpoint Detection and Response (Industrial CyberSecurity) and Endpoint Detection and Response Expert (on-premises) components are not compatible with each other.

The following conditions must be fulfilled for Endpoint Detection and Response Expert (on-premises) to work:

- OSMP (Open Single Management Platform) is installed.
- The application is activated and the functionality is covered by the license.
- The Endpoint Detection and Response Expert (on-premises) component is enabled.
- Application components that ensure the operation of EDR Expert (on-premises) are enabled and operational. The following components ensure the operation of EDR Expert (on-premises):
  - Real-Time File Protection
  - Exploit Prevention
  - Anti-Cryptor
  - AMSI Scanner
  - Kaspersky Security Network

Setting up EDR Expert (on-premises) Integration involves the following steps:

1. **Installing the Endpoint Detection and Response Expert (on-premises) component**

   In installation package settings or in the Setup Wizard, or by changing the set of application components in the Windows Control Panel, at the step when you must select application components for installation, select the following:

   - **Full functionality → Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** for the built-in agent
   - **Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** for the Endpoint Agent configuration

   To finish changing the set of application components, you must restart the computer.

2. **Endpoint Detection and Response Expert (on-premises) activation**

   You need to purchase a separate license for EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on).

   Licensing of the stand-alone Endpoint Detection and Response Expert (on-premises) functionality is the same as the licensing of Kaspersky Industrial CyberSecurity for Nodes. The functionality becomes available after adding a separate key for Kaspersky Endpoint Detection and Response (on-premises). As a result, two keys will be added on the computer: a key for Kaspersky Industrial CyberSecurity for Nodes and a key for Endpoint Detection and Response Expert (on-premises).

   Make sure that the Endpoint Detection and Response Expert (on-premises) functionality is included in the license.

3. **Connecting to telemetry collection server and response server**

Kaspersky Endpoint Detection and Response Expert (on-premises) requires a trusted connection between Kaspersky Endpoint Security and two servers:

- A *telemetry collection server* is a server that is part of a SIEM solution that collects, normalizes, correlates, analyzes, and stores information about events occurring on the computer.
- A *response server* is a server for receiving and scanning data, studying the behavior of objects, and publishing the results of such studies.

To configure a trusted connection, you must use a TLS certificate. You can get a TLS certificate on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help). Then you must add the TLS certificate to Kaspersky Industrial CyberSecurity for Nodes (see instructions below).

By default, Kaspersky Industrial CyberSecurity for Nodes checks only server TLS certificate. To make the connection more secure, you can additionally enable the verification of the computer on the server (two-way authentication). To enable this verification, you must turn on two-way authentication in the server and the Kaspersky Industrial CyberSecurity for Nodes settings. To use two-way authentication, you will also need a crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help).

How to connect a Kaspersky Industrial CyberSecurity for Nodes computer to EDR Expert (on-premises) using the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Configure** button.

   The **Endpoint Detection and Response Expert (on-premises)** window opens.
6. Select the **Enable Endpoint Detection and Response Expert (on-premises)** check box.
7. Select the **Endpoint Detection and Response Expert (version 8.0 or later)** mode.
8. Configure the telemetry collection servers connection:

   a. In the **Connection to telemetry collection servers** block, click the **Settings for connecting to KATA servers** link.

   b. In the window that opens, configure the connection to the telemetry collection servers:

   - **Timeout (sec)**. Maximum server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different server.
   - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the server. You can get a TLS certificate on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help).

- **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and the server. To use two-way authentication, you need to enable two-way authentication in the server settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help). After configuring the server settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

  The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

c. Click **OK**.

d. Add telemetry collection servers. To do this, specify the server address (IPv4, IPv6) and the port to connect to the server.

   You can add multiple telemetry collection server addresses. Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection with the server at the first IP address. If a connection cannot be established, Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection at the second IP address in the list and so on.

e. If necessary, configure telemetry.

9. Configure the response servers connection:

a. In the **Connection to response servers** block, configure the **Send sync request to server every (min)** setting. Frequency of synchronization requests sent to the server. During the synchronization, Kaspersky Industrial CyberSecurity for Nodes receives threat response tasks and sends task results.

b. Click the **Settings for connecting to KATA servers** link.

c. In the window that opens, configure the connection to the response servers:

- **Timeout (sec)**. Maximum server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different server.

- **Server TLS certificate**. TLS certificate for establishing a trusted connection with the server. You can get a TLS certificate on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help).

- **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and the server. To use two-way authentication, you need to enable two-way authentication in the server settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container on the Open Single Management Platform (see instructions in the Kaspersky Endpoint Detection and Response Expert (on-premises) Help). After configuring the server settings, you need to also enable two-way authentication in Kaspersky Endpoint Security settings and load a password-protected crypto-container.

  The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

d. Click **OK**.

e. Add response servers. To do this, specify the server address (IPv4, IPv6) and the port to connect to the server.

You can add multiple telemetry collection server addresses. Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection with the server at the first IP address. If a connection cannot be established, Kaspersky Industrial CyberSecurity for Nodes attempts to establish a connection at the second IP address in the list and so on.

10. Save your changes. To apply the policy on computers, close the padlocks.

As a result, the computer is added on the Open Single Management Platform (OSMP).

Configuring EDR Expert (on-premises) telemetry settings

Telemetry is a list of events that have occurred on the protected computer. Kaspersky Industrial CyberSecurity for Nodes analyzes telemetry data and sends it to telemetry collection servers during synchronization. For more information about transmitted telemetry events, see the Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Telemetry events arrive on the server almost continuously. Kaspersky Industrial CyberSecurity for Nodes initiates synchronization with the server when any of the following conditions are satisfied:

- Synchronization interval has run out.
- The number of events in the buffer exceeds the upper limit.

Therefore, by default, the application synchronizes every 30 seconds or whenever the buffer holds 1024 events. You can configure the synchronization behavior in the Kaspersky Industrial CyberSecurity for Nodes policy and select optimum values to match your network load (see instructions below).

If there is no connection between Kaspersky Industrial CyberSecurity for Nodes and the server, the application queues new events. When the connection is restored, Kaspersky Industrial CyberSecurity for Nodes sends queued events to the server in proper order. To avoid overloading the server, Kaspersky Industrial CyberSecurity for Nodes may skip some events. To enable this, you can optimize event transmission settings, for example, to set a maximum events-per-hour value (see instructions below).

To configure telemetry settings, perform the following steps:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Endpoint Detection and Response Expert (on-premises)** block, click the **Configure** button.

   The **Endpoint Detection and Response Expert (on-premises)** window opens.
6. Make sure that the **Send telemetry to telemetry collection servers** check box is selected in the **Data transmission settings** block.

7. If necessary, select the **Send telemetry with IOA only** check box. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the streaming scan technology, which allows real time tracking of such events.

8. If necessary, configure the synchronization with the server settings in the **Data transmission settings** block:

   - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the synchronization interval expires. The default setting is 30 seconds.

   - **Manage the number of event packages transmitted as part of a transaction**. The application synchronizes with the server when the buffer is filled with events. The default setting is 1024 events.

9. If necessary, clear the **Enable throttling** check box in the **Throttling** block.

   This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events. This option is enabled by default.

10. Configure optimization settings for sending events to the server:

    - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

    - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.

11. In the **Connection to response servers** block, enter a value for the **Send sync request to server every (min)** parameter.

12. Frequency of synchronization requests sent to the server. During synchronization, Kaspersky Industrial CyberSecurity for Nodes sends information about modified application settings and tasks.

13. Save your changes. To apply the policy on computers, close the padlocks .

EDR Expert (on-premises) telemetry exclusions

To improve performance and optimize data transmission to the Telemetry collection server, you can configure telemetry exclusions. For example, you can choose not to send network communications data for individual applications.

Kaspersky Industrial CyberSecurity for Nodes supports up to 10,000 EDR Expert (on-premises) inclusion and exclusion event filtering rules in total.

EDR Expert (on-premises) event filtering rules will not be passed from the policy to managed devices running Kaspersky Industrial CyberSecurity for Nodes version 4.5 or earlier if the supported limit for stored filtering rules is exceeded. The application will display a corresponding warning.

To create a telemetry exclusion in the Web Console:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Supplementary** section.
5. In the **Telemetry settings** block, click the **Configure** button.
6. Select the **EDR Expert (on-premises) telemetry** tab.
7. In the **General exclusions** block, click the **Add** button.

   The **Add exclusion rule** window opens.
8. If necessary, change the status of the rule. By default, the rule is enabled.
9. Enter a name for the rule.
10. Select the action to be performed when the rule is triggered:

    - **Do not collect**. The filtered event will be excluded from the sent telemetry.
    - **Exclude IOA**. The IOA rule trigger event will be excluded from the sent telemetry.
11. If the **Exclude IOA** option is selected, specify the IOA rules to be added to exclusions:

    - **Exclude all**. When the specified condition is met, the application will exclude events generated based on all IOA rules from the telemetry.
    - **Exclude by GUID**. Specify the GUID of the IOA rule. You can specify multiple GUIDs by using `,`. For more details on the IOA rules, please refer to the EDR Expert (on-premises) Help.

12. Specify the filtering condition:

    a. Select the field name to be used for filtering.

    b. Select an operator (see the table below) and specify the value against which the field value from the event will be compared.

List of conditional operators

Operator	Description
<	If the field value is less than the value specified in the condition, the event will be filtered out.
≤	If the field value is less than or equal to the value specified in the condition, the event will be filtered out.
=	If the value of the field is equal to the value specified in the condition, the event will be filtered out.
≥	If the value of the field is greater than or equal to the value specified in the condition, the event will be filtered out.
>	If the field value is greater than the value specified in the condition, the event will be filtered out.
≠	If the value of the field is not equal to the value specified in the condition, the event will be filtered out.
is like	If the field value matches the mask specified in the condition, the event will be filtered out. The application supports the `*` and `?` characters when entering a mask:
is not like	If the field value does not match the mask specified in the condition, the event will be filtered out. The application supports the `*` and `?` characters when entering a mask:
one of	If the field value matches one of the values in the list specified in the condition, the event is considered filtered.
none of	If the field value does not match any of the values in the list specified in the condition, the event is considered filtered.
is like one of	If the field value matches one of the masks specified in the condition, the event will be filtered out. The application supports the * and ? characters when entering a mask.
is not like one of	If the field value does not match any of the masks specified in the condition, the event will be filtered out. The application supports the * and ? characters when entering a mask.
exists	If the field specified in the condition is present in the event, the event will be filtered out.
not exists	If the field specified in the condition is not present in the event, the event will be filtered out.
contains	If the value specified in the condition is present in the field value, the event will be filtered out.
is equal to	If the value of the field is equal to the value specified in the condition, the event will be filtered out. The scan is case-insensitive.
bitwise AND	If the result of the Bitwise AND (&) operation between the field value and the value specified in the condition is 1, the event will be filtered out.

13. If necessary, you can create complex filter criteria by adding multiple filter conditions and groups of conditions. You can also add nested conditions and condition groups to a condition group. You can use the following operators:

    - **AND** means that the filter selects events that meet all of the specified conditions.
    - **OR** means that the filter selects events that meet one of the specified conditions.
    - **NOT** (to use this operator, select the **Add NOT before** option) means that the filter selects events that do not meet any of the specified conditions.

    Conditions and first-level condition groups are combined with the **AND** operator.

14. If your computer is running the Open Single Management Platform (OSMP), you can scan the filtering rule you created. To run the scan, click the **Check rule** button.

    In the window that opens, a table of events filtered by the created rule will be displayed. For more details, please refer to the EDR Expert (on-premises) Help.

15. If necessary, under **All event types**, add telemetry exclusions by event type.

    a. Click the event type name.

    b. In the window that opens, click the **Set up manually** button.

    c. If necessary, configure telemetry transmission for the selected event type using the **Send event** toggle switch. By default, telemetry transmission is enabled for all event types.

    d. In the **Exclusion rules** block, click the **Add** button.

    The **Add exclusion rule** window opens.

    e. Perform the actions described in steps 7–13 for each rule you add.

16. For some event types, you can also add inclusion rules to expand the telemetry collected:

    a. In the **Exclusion rules** block, click the **Add** button.

    The **Add inclusion rules** window opens.

    b. Enter a name for the rule.

    c. Under **Condition**, enter values for the displayed fields. The type of fields available depends on the selected event.

    Exclusion rules are prioritized over inclusion rules.

17. Save your changes. To apply the policy on computers, close the padlocks.

Exporting and importing EDR Expert (on-premises) event filters

Kaspersky Industrial CyberSecurity for Nodes supports up to 10,000 EDR Expert (on-premises) inclusion and exclusion event filtering rules in total.

EDR Expert (on-premises) event filtering rules will not be passed from the policy to managed devices running Kaspersky Industrial CyberSecurity for Nodes version 4.5 or earlier if the supported limit for stored filtering rules is exceeded. The application will display a corresponding warning.

You can export the list of exclusions to a JSON file. Then you can modify the file to, for example, add a large number of event IDs. You can also use the export and import function to back up the event filters or to migrate the list to a different server.

How to export and import event filters in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, go to the **Supplementary** section.

4. In the **Telemetry settings for EDR Expert (on-premises)** block, click the **Settings** button.

5. To export EDR Expert (on-premises) telemetry settings:

   a. Click **Export**.

   b. In the window that opens, specify the name of the JSON file to which you want to export the settings, and select the folder in which you want to save this file.

   c. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the settings to the JSON file.

6. To import telemetry settings:

   a. Click **Import**.

   b. Select the JSON file from which you want to import the event filters.

   c. Open the file.

   d. In the displayed dialog box, confirm the modification of EDR Expert (on-premises) telemetry settings.

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

How to export and import event filters in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to the **Supplementary** section.

5. In the **Telemetry settings** block, click the **Configure** button.

6. Select the **EDR Expert (on-premises) telemetry** tab.

7. Click **Export** to export EDR Expert (on-premises) telemetry settings.

   Kaspersky Industrial CyberSecurity for Nodes saves a file named filterExport.json in the standard download folder.

8. To import telemetry settings:

   a. Click **Import**.

   b. Select the JSON file from which you want to import the event filters.

   c. Open the file.

   d. Select how you want event filtering rules to be imported: by adding to existing rules or by discarding existing rules and replacing with new ones.

e. Save your changes.

The rules contained in the JSON file will be displayed in the list.

How to export and import event filters in the Application Console

1. In the Application Console tree, select the **Telemetry settings** node.
2. In the **Telemetry settings for EDR Expert (on-premises)** block, click the **Settings** button.
3. To export EDR Expert (on-premises) telemetry settings:
   a. Click **Export**.
   b. In the window that opens, specify the name of the JSON file to which you want to export the settings, and select the folder in which you want to save this file.
   c. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the settings to the JSON file.
4. To import telemetry settings:
   a. Click **Import**.
   b. Select the JSON file from which you want to import the event filters.
   c. Open the file.
   d. In the displayed dialog box, confirm the modification of EDR Expert (on-premises) telemetry settings.
5. Click **OK** to save the changes.

You can also export or import event filters on the command line.

YARA Scan

A *YARA scan* is a process wherein Kaspersky Industrial CyberSecurity for Nodes uses YARA files to look for signatures of malicious activity on devices. The scan is performed recursively on local disks. Scanning of network, removable, and cloud resources is not supported.

To run a YARA scan, you need a current license for EDR Expert (on-premise).

YARA files are files with the .YARA or .YAR extensions that contain YARA rules. A *YARA rule* describes signatures of targeted attacks and intrusions into the corporate IT infrastructure. Kaspersky Industrial CyberSecurity for Nodes uses these rules to scan objects. If an object matches a rule, the analyzer diagnoses an infection and logs the details in the log.

Take into account the following requirements and limitations involved in using YARA files:

- Kaspersky Industrial CyberSecurity for Nodes supports YARA files with the .YARA or .YAR extensions that follow the YARA 4.2.3 open standard for describing indicators of compromise.
- If you run a YARA scan using YARA files that are not supported by Kaspersky Industrial CyberSecurity for Nodes or contain syntax errors, the scan is aborted with the corresponding error notification.
- The IDs of YARA files used in a YARA Scan task must be unique. If there are YARA files with the same identifier, it might affect the task execution results.
- A YARA scan is aborted after 128 matches with indicators described in YARA rules. This is necessary to limit the number of entries in the YARA scan report to make it easier to analyze and to protect the report from overflowing because of imprecisely formulated YARA rules that may generate a vast number of matches.

We recommend creating one rule per YARA file. This approach improves the readability of YARA scan results.

You can only run a YARA scan using the command line interface.

A YARA scan can take a long time. Depending on the drive size, task settings, and the number of objects on the disk, a YARA scan can last anywhere from several minutes to several hours. The application does not display a progress indicator. It is not possible to stop or cancel a YARA scan. You are advised to wait until the results of a YARA scan are available.

If the command has completed successfully (return value `0`) and it detected indicators of compromise, Kaspersky Industrial CyberSecurity for Nodes outputs the following task result information to the command line:

`Started at <time>` `Finished at <time>`	Start time and completion time of a scan.
`Host name: <computer name>`	The name of the computer on which the object was detected.
`Result: <error>`	Error code for the error that occurred while running the task. If there are no errors, the application outputs `0x00000000`.
`Comment: <comment text>`	Error description for the error that occurred while running the task. For example, `Operation timeout`.
`Object Name:` or `Process:` (when scanning process memory)	The name of the object or process on which the YARA rule triggered.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashes of the object on which the YARA rule triggered.
`Rule Name`	The name of the triggered YARA rule.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadata specified in the YARA rule.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Found matches within the object that meet the YARA rule conditions:
	• Offset in the process memory or file where a match was detected (`Offset`).
	• The name of the matching string in the YARA rule (`String name`).
	• The matching string in the process memory or file (`String data`).

EDR telemetry exclusions

To improve performance and optimize data transmission to the Telemetry collection server, you can configure telemetry exclusions. For example, you can choose not to send network communications data for individual applications.

Creating EDR telemetry exclusions in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Supplementary → Telemetry settings for KATA Integration / Integration with KICS for Networks** and click **Settings**.
4. In the window that opens, configure telemetry exclusions (see the table below).
5. Save your changes.

Creating EDR telemetry exclusions in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Supplementary → Telemetry settings for KATA Integration / Integration with KICS for Networks** and click the **Configure** button.
5. In the window that opens, configure telemetry exclusions (see the table below).
6. Save your changes.

Creating EDR telemetry exclusions in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and select **Telemetry settings for KATA Integration / Integration with KICS for Networks** from the context menu of the node.
2. In the window that opens, configure telemetry exclusions (see the table below).
3. Save your changes.

Telemetry exclusion parameters

Parameter	Description
Excluded processes	**Optimize the telemetry size to send**. Kaspersky Industrial CyberSecurity for Nodes allows optimizing the amount of transmitted data and excluding events with certain codes from telemetry: code 102 (basic communications) and 8 (network activity of the process) for the Microsoft SMB protocol, the WinRM service, and the klnagent.exe process of the Network Agent, as well as extended information about the types of network packets for all types of network protocols. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system. **Use for the following event types**: • **File modification**. • **Network events**. • **Process: console interactive input**. • **Module loaded**. • **Registry modified**. • **DNS logs**. • **Process access**. • **Code injection**. • **WMI query**. • **Pipe**. • **LDAP**. • **AMSI**.
Excluded network communications	• **Rule name**. Name of the rule. • **Direction**. Incoming or outgoing events. • **Protocol**. Protocol type. • **Raw socket**. Whether to use a raw socket. • **Protocol number**. Protocol number. • **TLS certificate**. Digital certificate that is used to encrypt the connection between the client and the server using the TLS protocol. • **Local port or range**. Specific port or a range of possible local ports. • **Remote port or range**. Specific port or a range of possible remote ports. • **Local address**. The network address of the computer for which Kaspersky Industrial CyberSecurity for Nodes is excluding telemetry from network traffic. • **Remote address**. The network address of the computer for which Kaspersky Industrial CyberSecurity for Nodes is excluding telemetry from network traffic. Only the IPv4 format is supported for IP addresses. • **Applications**. List of executable files of applications for which Kaspersky Industrial CyberSecurity for Nodes is excluding EDR telemetry from network traffic.
Excluded file operations	• **Rule name**. Name of the rule. • **File name or mask**. Name or mask of a file or folder; Kaspersky Industrial CyberSecurity for Nodes applies the exclusion rule when this file or folder is accessed. Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a mask: • **Operation type**. Type of file operations, for example, create file or edit file attributes. • **Previous path**. Previous path to the file. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND.

Parameter	Description
	Process details and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Parent path**. Path to the folder containing the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded DNS operations	• **Rule name**. Name of the rule. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system. **DNS**: • **DNS server IP address**. Address of the server that processes DNS queries. • **Query options**. Parameters that regulate the format and condition of the DNS query. • **Status**. Current status of the DNS operation. • **Domain name**. Domain name for which the query is being processed. • **Settings type ID**. Unique ID of the DNS settings type. • **Response data**. Data returned by the server in response to the DNS query.
Excluded LDAP operations	• **Rule name**. Name of the rule. • **LDAP search scope**. Scope in which the LDAP search is being performed. • **Filter**. Search criteria for filtering LDAP objects. • **Distinguished name for LDAP objects search**. Unique name of the object for the LDAP search. • **Object attributes**. Properties of objects that will be extracted in the LDAP query. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256.

Parameter	Description
	You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.

Parameter	Description
Excluded process access queries	**Rule name**. Name of the rule. **Operation type**. Type of process access operation, for example, "any" or "open". **Requested access to the process**. Level of access to the process. **Call stack trace**. Information about the sequence of function calls related to access to the process. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details**, **Parent process details**, **File of the target process**, **Handle to the source process** and **Handle to the target process**. • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded code injections	• **Rule name**. Name of the rule. • **Access method**. Access method used for the code injection. • **Call stack**. Function call sequence related to the code injection. • **Modified command line**. Command line that was modified by the injection. • **Injection address**. Memory location where the injection took place. • **Injected DLL name**. Name of the dynamic-link library (DLL) used for the injection. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded WMI queries	• **Rule name**. Name of the rule. • **WMI operation type**. Type of operation performed using WMI. • **Remote query**. Information on whether the WMI query was executed remotely. • **Name of a computer that executed a WMI command**. Name of the computer that initiated the query. • **WMI user account**. User account that was used for the WMI query. • **Executed WMI command**. Specific command executed via WMI. • **WMI namespace**. Namespace in which the WMI operation was performed. • **WMI event consumer filter**. Filter that is used to process events in WMI. • **Name of the created WMI event consumer**. Name of the event consumer created using WMI. • **Source code of a WMI event consumer**. Code used to create a WMI event consumer. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND.

Parameter	Description
	Process details and **Parent process details:** • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded pipe operations	• **Rule name**. Name of the rule. • **Pipe name**. Name of the pipe. • **Operation type**. Type of operations with pipes, for example, creation or connection. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256. You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded registry changes	• **Rule name**. Name of the rule. • **Operation type**. Type of operation performed with the registry, for example, add, delete, modify. • **Path**. Path to the registry key in which the changes took place. • **Value name**. Name of the registry value that was modified. • **Value**. New or modified registry value. • **Full name of a registry file**. Full path to the registry file in which the modifications were made. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND. **Process details** and **Parent process details**: • **Full path**. Full path to the file including its name and extension. Kaspersky Industrial CyberSecurity for Nodes supports environment variables and the `*` and `?` characters when entering a mask: • **Command line text**. Command used to run the file. • **Description**. Value of the FileDescription parameter from a RT_VERSION (VersionInfo) resource. • **Original file name**. Value of the OriginalFilename parameter from a RT_VERSION (VersionInfo) resource. • **Version**. Value of the FileVersion parameter from a RT_VERSION (VersionInfo) resource. • **File checksums**. MD5 and SHA256.

Parameter	Description
	You can also select a file manually, and the application will automatically fill out the fields from the selected file. In 64-bit operating systems, you must manually enter the parameters of the 64-bit version of the executable file of a process from the `C:\windows\system32` folder because the application populates the executable file parameter fields with data from the properties of the 32-bit version of the same executable file in the `C:\windows\syswow64` folder. For example, if you select `C:\windows\system32\cmd.exe`, the plug-in displays the parameters of `C:\windows\syswow64\cmd.exe`. Such behavior is dictated by peculiarities of the operating system.
Excluded operations with devices	• **Rule name**. Name of the rule. • **Device type**. Device type: local printer, removable drive, CD/DVD drive, etc. For details, see Device Access Rules. • **Device ID**. Unique ID that can be used to identify the specific instance of the device. • **Device name**. Name of the device. Kaspersky Industrial CyberSecurity for Nodes combines rule triggering criteria with a logical AND.

Kaspersky Industrial CyberSecurity for Networks Integration

Kaspersky Industrial CyberSecurity for Networks is designed to protect the infrastructure of industrial enterprises from information security threats and to ensure the continuity of technological processes. Kaspersky Industrial CyberSecurity for Networks analyzes industrial network traffic to detect deviations in the values of technological parameters, detect signs of network attacks, and monitor the operation and current state of devices on the network. The application is a part of the Kaspersky Industrial CyberSecurity solution. For full information about Kaspersky Industrial CyberSecurity for Networks, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

Kaspersky Industrial CyberSecurity for Nodes supports integration with Kaspersky Industrial CyberSecurity for Networks. Data about events on the device, received by Kaspersky Industrial CyberSecurity for Nodes, is sent to Kaspersky Industrial CyberSecurity for Networks server. Integration between the applications enhances Kaspersky Industrial CyberSecurity for Networks capabilities to investigate and respond to threats in industrial networks.

Kaspersky Industrial CyberSecurity for Nodes configurations for integration with Kaspersky Industrial CyberSecurity for Networks

The following configurations are possible:

- **[KICS+built-in agent]**. In this configuration, Kaspersky Industrial CyberSecurity for Nodes acts as both the application that ensures the security of the computer and the application for working with Kaspersky Industrial CyberSecurity for Networks. The built-in agent is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.

- **[Third-party EPP+KICS in Endpoint Agent mode]**. In this configuration, the security of the computer is provided by the third-party Endpoint Protection Platform (EPP). Integration with Kaspersky Industrial CyberSecurity for Networks is provided by Kaspersky Industrial CyberSecurity for Nodes in Endpoint Agent mode. The Endpoint Agent mode is available in Kaspersky Industrial CyberSecurity for Nodes starting with version 4.5.

For integration of Kaspersky Industrial CyberSecurity for Nodes built-in agent with Kaspersky Industrial CyberSecurity for Networks, the following conditions must be satisfied:

- Kaspersky Industrial CyberSecurity for Networks is deployed.
- Kaspersky Security Center version 14.2 or higher is deployed.
- The following protection components are enabled and functioning: Exploit Prevention, Remediation Engine, Anti-Cryptor.

To integrate the Endpoint Agent configuration with Kaspersky Industrial CyberSecurity for Networks, the following must be deployed:

- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center version 14.2 or higher.

Support for previous versions of Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes 4.5 supports integration with Kaspersky Industrial CyberSecurity for Networks using the built-in agent or the Endpoint Agent mode; you do not need to install Kaspersky Endpoint Agent.

If you are using Kaspersky Industrial CyberSecurity for Nodes older than 4.5 for integration with Kaspersky Industrial CyberSecurity for Networks, you must install Kaspersky Endpoint Agent separately.

Configuring integration with Kaspersky Industrial CyberSecurity for Networks

Integration with Kaspersky Industrial CyberSecurity for Networks involves the following steps:

1. **Installing the Kaspersky Industrial CyberSecurity for Networks Integration component**

   In installation package settings or in the Setup Wizard, or by changing the set of application components in the Windows Control Panel, at the step when you must select application components for installation, select the following:

   - **Full functionality → Endpoint Agent → Integration with KICS for Networks** for the built-in agent
   - **Endpoint Agent → Integration with KICS for Networks** for the Endpoint Agent mode

   > To finish changing the set of application components, you must restart the computer.

2. **Activating the Kaspersky Industrial CyberSecurity for Networks Integration component**

   Make sure that your license covers the Activating the Kaspersky Industrial CyberSecurity for Networks Integration functionality.

3. **Enabling and configuring the Kaspersky Industrial CyberSecurity for Networks Integration component**

Kaspersky Industrial CyberSecurity for Nodes supports TCP and UDP protocols for sending telemetry to the KICS for Networks server. Depending on the settings of the KICS for Networks integration server you are connecting to, you need to select the corresponding protocol and specify the connection settings. For more details on integration server settings, refer to the KICS for Networks Help.

The application also supports integration with KICS for Networks in a network with a data diode. A data diode is an unidirectional gateway for communication between protected network segments and external devices. The application can send telemetry via a data diode using the following protocols:

- MQTT
- UDP

For more details about sending telemetry to KICS for Networks via data diodes, see the KICS for Networks Help.

Kaspersky Industrial CyberSecurity for Nodes supports software MQTT servers (for example, Mosquitto) as an MQTT broker. You can use the application in both subscriber and publisher modes. The application, operating in MQTT publisher mode, sends telemetry via a data diode to the MQTT broker.

Telemetry sent to the MQTT broker server may contain confidential information. To control access to data, you must take steps to ensure the security of telemetry.

How to configure the integration with Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Telemetry collection servers** section.
4. In the **Integration with KICS for Networks** block, click the **Settings** button.

   The **Integration with KICS for Networks** window opens.
5. Select the **Integration with KICS for Networks** check box.
6. On the **General** tab, select the telemetry mode:

   - **Send telemetry to KICS for Networks server via the TCP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry directly to the Kaspersky Industrial CyberSecurity for Networks server via the TCP protocol.
   - **Send telemetry to a data diode as an MQTT publisher**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the MQTT broker server that is built into the software data diode.
   - **Send telemetry to KICS for Networks server via the UDP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the Kaspersky Industrial CyberSecurity for Networks server through a data diode via the UDP protocol.

7. For the **Send telemetry to KICS for Networks server via the TCP protocol** mode, manage the following settings:

   - **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry. Range of possible port values: 1–65535. The default port is 8081.

   - **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.

   - **Server connection settings**. Manage the following settings:

     - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.

     - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.

     - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

       The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

8. For the **Send telemetry to a data diode as an MQTT publisher** mode, manage the following settings:

   a. Click **Server connection settings**.

   b. Enter credentials for authentication at the MQTT broker server.

   c. Enter the IP address and port of the MQTT broker server.

9. For the **Send telemetry to KICS for Networks server via the UDP protocol** mode, manage the following settings:

   a. Enter the IP address and port of server.

   b. To enable data encryption, click the **Server connection settings** button and select the **Use encryption when sending data via the UDP protocol** check box.

      You need to evaluate whether encryption of the transmitted data is necessary.

   c. Enter the encryption key password and upload the encryption key file with the .PEM extension.

10. Go to the **Data transmission** tab.

11. Configure data transfer settings:

    - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

      When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

    - **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

    - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

    - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

    If necessary, configure telemetry in promiscuous mode. By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

    Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

    a. On the **Telemetry collection** tab, select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

    b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

    c. If necessary, create a list of subnets.

12. Save your changes.

How to configure the integration with Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Integration with KICS for Networks** block, click the **Configure** button.

   The **Integration with KICS for Networks** window opens.
6. Select the **Enable Integration with KICS for Networks** check box.
7. Under **Connection settings**, select the telemetry mode:

   - **Send telemetry to KICS for Networks server via the TCP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry directly to the Kaspersky Industrial CyberSecurity for Networks server via the TCP protocol.
   - **Send telemetry to a data diode as an MQTT publisher**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the MQTT broker server that is built into the software data diode.
   - **Send telemetry to KICS for Networks server via the UDP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the Kaspersky Industrial CyberSecurity for Networks server through a data diode via the UDP protocol.
8. For the **Send telemetry to KICS for Networks server via the TCP protocol** mode, manage the following settings:

   - **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry. Range of possible port values: 1–65535. The default port is 8081.
   - **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.
   - **Server connection settings**. Manage the following settings:

     - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.
     - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.

- **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

  The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

9. For the **Send telemetry to a data diode as an MQTT publisher** mode, manage the following settings:

   a. Enter credentials for authentication at the MQTT broker server.

   b. Enter the IP address and port of the MQTT broker server.

10. For the **Send telemetry to KICS for Networks server via the UDP protocol** mode, manage the following settings:

    a. Enter the IP address and port of server.

    b. To enable data encryption, click the **Server connection settings** button and select the **Use encryption when sending data via the UDP protocol** check box.

    > You need to evaluate whether encryption of the transmitted data is necessary.

    c. Enter the encryption key password and upload the encryption key file with the .PEM extension.

11. Configure data transfer settings:

    - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

      > When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

    - **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

- **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

- **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

If necessary, configure telemetry in promiscuous mode. By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

> Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

a. Select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

c. If necessary, create a list of subnets.

12. Save your changes.

How to configure the integration with Kaspersky Industrial CyberSecurity for Networks in the Application Console

1. In the Application Console tree, select the **Telemetry collection servers → Integration with KICS for Networks** section.

2. Click the **Properties** link in the results pane.

   The **Properties: Integration with KICS for Networks** window opens on the **General** tab.

3. Select the **Integration with KICS for Networks** check box.

4. On the **General** tab, select the telemetry mode:

   - **Send telemetry to KICS for Networks server via the TCP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry directly to the Kaspersky Industrial CyberSecurity for Networks server via the TCP protocol.

   - **Send telemetry to a data diode as an MQTT publisher**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the MQTT broker server that is built into the software data diode.

   - **Send telemetry to KICS for Networks server via the UDP protocol**. Kaspersky Industrial CyberSecurity for Nodes sends telemetry to the Kaspersky Industrial CyberSecurity for Networks server through a data diode via the UDP protocol.

5. For the **Send telemetry to KICS for Networks server via the TCP protocol** mode, manage the following settings:

   - **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry. Range of possible port values: 1–65535. The default port is 8081.

   - **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.

   - **Server connection settings**. Manage the following settings:

     - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.

     - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.

     - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

       The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

6. For the **Send telemetry to a data diode as an MQTT publisher** mode, manage the following settings:

   a. Click **Server connection settings**.

   b. Enter credentials for authentication at the MQTT broker server.

   c. Enter the IP address and port of the MQTT broker server.

7. For the **Send telemetry to KICS for Networks server via the UDP protocol** mode, manage the following settings:

   a. Enter the IP address and port of server.

   b. To enable data encryption, click the **Server connection settings** button and select the **Use encryption when sending data via the UDP protocol** check box.

   > You need to evaluate whether encryption of the transmitted data is necessary.

   c. Enter the encryption key password and upload the encryption key file with the .PEM extension.

8. Go to the **Data transmission** tab.

9. Configure data transfer settings:

   - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

     > When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

   - **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

   - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

   - **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

   If necessary, configure telemetry in promiscuous mode. By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

a. On the **Telemetry collection** tab, select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

c. If necessary, create a list of subnets.

10. Save your changes.

You can also configure Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber. In this mode, the application receives telemetry from the MQTT broker through a data diode and then forwards the telemetry to KICS for Networks.

How to configure the application as an MQTT subscriber in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the group to which the computer belongs.
2. In the results pane, select the **Devices** tab.
3. Double-click to open the computer properties window.
4. Go to the **Applications** section.
5. In the list of Kaspersky applications installed on the computer, select Kaspersky Industrial CyberSecurity for Nodes and double-click to open the application properties.
6. Select the **Telemetry collection servers** section.
7. In the **Integration with KICS for Networks** block, click the **Settings** button.

   The **Integration with KICS for Networks** window opens.
8. Select the **Integration with KICS for Networks** check box.
9. On the **General** tab, select **Send telemetry to KICS for Networks server via the TCP protocol**.
10. Manage the following settings:

    - **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry.
    - **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.

- **Server connection settings**. Manage the following settings:

  - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.

  - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.

  - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

    The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

- Select the **Receive telemetry from a data diode as an MQTT subscriber** check box.

- Enter credentials for authentication at the MQTT broker server.

- Enter the IP address and port of the MQTT broker server.

11. Go to the **Data transmission** tab.

12. Configure data transfer settings:

    - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

      When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

    - **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

- **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

- **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

13. If necessary, configure telemetry in promiscuous mode.

    By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

    Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

    a. On the **Telemetry collection** tab, select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

    b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

    c. If necessary, create a list of subnets.

14. Save your changes.

How to configure the application as an MQTT subscriber in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.

2. Click a computer name.

3. In the displayed computer properties window, select the **Applications** tab.

4. Click **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

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

6. Select the **Telemetry collection servers** section.

7. In the **Integration with KICS for Networks** block, click the **Configure** button.

   The **Integration with KICS for Networks** window opens.

8. Select the **Integration with KICS for Networks** check box.

9. On the **General** tab, select **Send telemetry to KICS for Networks server via the TCP protocol**.

10. Manage the following settings:

    - **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry.

    - **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.

    - **Server connection settings**. Manage the following settings:

      - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.

      - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.

      - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

        The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

    - Select the **Receive telemetry from a data diode as an MQTT subscriber** check box.

    - Enter credentials for authentication at the MQTT broker server.

    - Enter the IP address and port of the MQTT broker server.

11. Configure data transfer settings:

    - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

      When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

- **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

- **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

- **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

12. If necessary, configure telemetry in promiscuous mode.

    By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

    > Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

    a. Select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

    b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

    c. If necessary, create a list of subnets.

13. Save your changes.

How to configure the application as an MQTT subscriber in the Application Console

1. In the Application Console tree, select the **Telemetry collection servers → Integration with KICS for Networks** section.

2. Click the **Properties** link in the results pane.

   The **Properties: Integration with KICS for Networks** window opens on the **General** tab.

3. Select the **Integration with KICS for Networks** check box.

4. On the **General** tab, select **Send telemetry to KICS for Networks server via the TCP protocol**.

5. Manage the following settings:

- **Address** and **Port**. IP address and port of the Kaspersky Industrial CyberSecurity for Networks server to which you want to send telemetry.
- **Interval between requests (min)**. The interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.
- **Server connection settings**. Manage the following settings:
  - **Timeout (sec)**. Maximum server response timeout. After the timeout, Kaspersky Industrial CyberSecurity for Nodes re-connects to the server. Range of available values: 1–60000 sec. The default value is 10 seconds.
  - **Server TLS certificate**. TLS certificate for establishing a trusted connection with the Kaspersky Industrial CyberSecurity for Networks server. You can get a TLS certificate using the Kaspersky Industrial CyberSecurity for Networks management interface.
  - **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks. To use two-way authentication, you need to enable two-way authentication in the Kaspersky Industrial CyberSecurity for Networks settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring the Kaspersky Industrial CyberSecurity for Networks settings, you need to also enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings and load a password-protected crypto-container.

    The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.
- Select the **Receive telemetry from a data diode as an MQTT subscriber** check box.
- Enter credentials for authentication at the MQTT broker server.
- Enter the IP address and port of the MQTT broker server.

6. Go to the **Data transmission** tab.

7. Configure data transfer settings:

- **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the specified time. Range of available values: 1–3600 sec. The default value is 30 seconds.

  When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **Maximum event transmission delay (sec)** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.

- **Enable request throttling**. This feature helps optimize the load on the server. If the check box is selected, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Industrial CyberSecurity for Nodes stops sending events.

- **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Industrial CyberSecurity for Nodes resumes sending events after an hour. Range of available values: 10–65535. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

- **Percentage of event limit excess**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Industrial CyberSecurity for Nodes resumes sending events when the ratio of other events to the total number of events becomes big enough again. Range of available values: 5–100%. The default value is 15%

8. If necessary, configure telemetry in promiscuous mode.

   By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry.

   > Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.

   a. On the **Telemetry collection** tab, select the **Enable Promiscuous mode for the application and host network interfaces** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for all network interfaces of the computer on which the application is installed.

   b. Select the **Use in Promiscuous mode only host network interfaces configured for the specified subnets** check box if you want to enable the promiscuous mode of network traffic collection from all available subnets for network interfaces configured for subnets from the list below.

   c. If necessary, create a list of subnets.

9. Save your changes.

If necessary, you can configure integration with Kaspersky Industrial CyberSecurity for Networks using the command line interface.

Special considerations and limitations of the Kaspersky Industrial CyberSecurity for Networks integration

Modifying audit policy settings

For the integration with Kaspersky Industrial CyberSecurity for Networks to function correctly, you must modify the audit policy settings. The behavior of the application depends on whether the device belongs to a domain or not:

- If the device is not part of a domain, the application automatically modifies the local policy settings as needed.
- If the device belongs to a domain, the application does not modify domain group policy settings. You can exclude such a device from the domain or configure domain group policy settings manually:
  - For the **Audit User Account Management** subcategory, enable the **Success** setting.
  - For the **Audit Logon**, **Audit Logoff**, and **Audit Other Logon/Logoff Events** subcategories, enable the **Success** and **Failure** settings.

Limitations of integration with Kaspersky Industrial CyberSecurity for Networks

The Kaspersky Industrial CyberSecurity for Networks integration functionality has the following limitations:

- On Windows XP computers, telemetry cannot be sent to the MQTT broker server.
- Delivery of messages received from the Kaspersky Industrial CyberSecurity for Nodes via the data diode is not guaranteed when there is no connection with the Kaspersky Industrial CyberSecurity for Networks server.
- The Wi-Fi network monitoring functionality is supported in networks that use the IPv4 protocol. Devices with IPv6 addresses will not be detected.
- For Wi-Fi networks with a hidden SSID, information about the used protection standards and encryption protocols, as well as roaming standards cannot be collected.
- When scanning Wi-Fi networks, the application uses the following protocols: DHCP, ICMP, ARP, mDNS, UPnP, and NetBIOS. For the application to work correctly, you need to allow the use of these protocols in your network.
- On protected devices running Windows 11, Windows Server 2025 and later, you must enable the Location services in the operating system settings to collect data about Wi-Fi networks. If Location services are turned off, Kaspersky Industrial CyberSecurity for Nodes does not collect or send data about Wi-Fi networks to Kaspersky Industrial CyberSecurity for Networks.
- Wi-Fi data collection is not available on devices running operating systems versions earlier than Windows Vista.

Configuring Wi-Fi network monitoring

You can configure the sending to the Kaspersky Industrial CyberSecurity for Networks server of data about Wi-Fi networks detected by a protected device running Kaspersky Industrial CyberSecurity for Nodes, as well as data about devices connected to the same Wi-Fi network as the protected device. Kaspersky Industrial CyberSecurity for Networks uses the collected data to perform centralized monitoring of Wi-Fi networks within your infrastructure. For more details, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

To reduce the load on network infrastructure, it is recommended to enable Wi-Fi data collection only on those devices that are necessary to ensure the completeness of the data collected.

You can configure the collection and transmission of Wi-Fi network data only in the Kaspersky Security Center Administration Console. Only current settings can be viewed in the Application Console.

How to configure the collection and transmission of Wi-Fi network data in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Telemetry collection servers** section.
4. In the **Integration with KICS for Networks** block, click the **Settings** button.
   The **Integration with KICS for Networks** window opens.
5. Go to the **Network and device discovery settings** tab.
6. Configure Wi-Fi network settings:
   - **Discover Wi-Fi networks**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes collects information about Wi-Fi networks available on the protected device and sends it to Kaspersky Industrial CyberSecurity for Networks. By default, the functionality is disabled.
   - **Discover wired and wireless devices in the connected network**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes collects information about devices connected to the same Wi-Fi network as the protected device and sends it to Kaspersky Industrial CyberSecurity for Networks. By default, the functionality is disabled.
7. If necessary, change the default settings for data collection and transmission:
   - **Run every (minutes)**. Specify the scan interval in minutes. Range of available values: 1–150 min. The default value is 5 minutes.
   - **Send data to server every (minutes)**. Specify the interval at which data is transmitted to the server in minutes. Range of available values: 1–150 min. The default value is 10 minutes.

     The scan interval must be shorter than the data transmission interval.

If the application performs multiple scans during a single data transmission interval, the collected data is aggregated according to the following rules:

- In the aggregated data, MAC addresses are used as unique identifiers for scanned objects.
- For each scanned object, the aggregated data includes the information obtained during the most recent scan of that interval.
- If the scanning device has switched between multiple Wi-Fi networks, the aggregated data will contain only the information collected from the most recent network for the current transmission interval.
- If the scanned object is no longer detected, the aggregated data will include the most recent information collected about it, along with the timestamp of the last detection.
- Data associated with the previous SSID is not retained when you change the SSID of a Wi-Fi network. The aggregated data contains only information related to the last SSID.

8. Save your changes.

How to configure the collection and sending of information about Wi-Fi networks in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Telemetry collection servers** section.
5. In the **Integration with KICS for Networks** block, click the **Configure** button.

   The **Integration with KICS for Networks** window opens.
6. Under **Network and device discovery settings**, configure Wi-Fi network settings:

   - **Discover Wi-Fi networks**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes collects information about Wi-Fi networks available on the protected device and sends it to Kaspersky Industrial CyberSecurity for Networks. By default, the functionality is disabled.
   - **Discover wired and wireless devices in the connected network**. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes collects information about devices connected to the same Wi-Fi network as the protected device and sends it to Kaspersky Industrial CyberSecurity for Networks. By default, the functionality is disabled.
7. If necessary, change the default settings for data collection and transmission:

   - **Run every (minutes)**. Specify the scan interval in minutes. Range of available values: 1–150 min. The default value is 5 minutes.
   - **Send data to server every (minutes)**. Specify the interval at which data is transmitted to the server in minutes. Range of available values: 1–150 min. The default value is 10 minutes.

   The scan interval must be shorter than the data transmission interval.

If the application performs multiple scans during a single data transmission interval, the collected data is aggregated according to the following rules:

- In the aggregated data, MAC addresses are used as unique identifiers for scanned objects.
- For each scanned object, the aggregated data includes the information obtained during the most recent scan of that interval.
- If the scanning device has switched between multiple Wi-Fi networks, the aggregated data will contain only the information collected from the most recent network for the current transmission interval.
- If the scanned object is no longer detected, the aggregated data will include the most recent information collected about it, along with the timestamp of the last detection.
- Data associated with the previous SSID is not retained when you change the SSID of a Wi-Fi network. The aggregated data contains only information related to the last SSID.

8. Save your changes.

Monitoring EDR actions

The *EDR action monitoring center* is a console in which you can view the Threat Response history for all Kaspersky Detection and Response solutions. If your organization has multiple Detection and Response deployed, Kaspersky Industrial CyberSecurity for Nodes displays Threat Response history for all solutions. This lets you analyze the performance of Detection and Response solutions on a separate computer and optimize the settings of these solutions.

The monitoring center provides the following information:

- Information about Threat Response tasks (for example, the *Terminate process* task)
- Changes of Network isolation and Execution prevention rules

If threat response encounters an error related to access to a network share, such an error is omitted from the displayed Threat Response history.

To open the EDR action monitoring center console.

1. In the main window of the Web Console, select **Asset management → Assets (Devices)**.
2. Click the name of the computer on which you want to view the threat response history.
   The computer properties window opens.
3. Select the **Applications** tab.
4. Click **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.
   This opens the local application settings.

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

6. Go to **Telemetry collection servers** → **Response history**.

This opens the EDR action monitoring center console. You can use the console to view Threat Response task statuses, task duration, rule changes, and initiator details.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent supports interaction between the application and other Kaspersky solutions for detecting advanced threats (e.g. Kaspersky Anti Targeted Attack Platform). Kaspersky solutions are compatible with specific versions of Kaspersky Endpoint Agent.

To use Kaspersky Endpoint Agent as part of Kaspersky solutions, you must activate those solutions with a corresponding license key.

Kaspersky Endpoint Agent supports interaction with the following Kaspersky solutions to detect sophisticated threats (such as targeted attacks):

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response (supports Kaspersky Endpoint Agent 3.9 and higher)
- Kaspersky Anti Targeted Attack Platform (supports Kaspersky Endpoint Agent 3.8 and higher)
- Kaspersky Managed Detection and Response

The Kaspersky Industrial CyberSecurity for Nodes 4.0 distribution kit includes the Kaspersky Endpoint Agent application; for earlier versions, you can request a Kaspersky Endpoint Agent distribution kit from your Technical Account Manager (TAM). Starting with version 4.5, the Kaspersky Industrial CyberSecurity for Nodes distribution kit does not include the Kaspersky Endpoint Agent distribution kit. Kaspersky Industrial CyberSecurity for Nodes 4.5 includes the built-in agent, which the application uses to support integration with Detection and Response solutions. You cannot install both applications on the same computer.

Migrating the [KICS+KEA] configuration to [KICS+built-in Enpoint Agent] configuration

Starting with version 4.5, Kaspersky Industrial CyberSecurity for Nodes includes the built-in agent to support Detection and Response solutions. You no longer need a separate Kaspersky Endpoint Agent application to work with these solutions. When you deploy Kaspersky Industrial CyberSecurity for Nodes on computers that have Kaspersky Endpoint Agent installed, Detection and Response solutions will continue working with Kaspersky Industrial CyberSecurity for Nodes, and the Kaspersky Endpoint Agent application is removed from the computer.

Migrating the [KICS+KEA] configuration to [KICS+built-in agent] involves the following steps:

1. **Upgrading Kaspersky Security Center**

   Upgrade all Kaspersky Security Center components to version 14.2 or higher, including Network Agent on user computers.

2. **Installing/upgrading Kaspersky Industrial CyberSecurity for Nodes to version 5.0**

   If you are installing the application, in the installation package settings or in the Setup Wizard, along with other required components, select **Full functionality → Endpoint Agent**.

   If you update the application, Kaspersky Industrial CyberSecurity for Nodes supports automatic component selection on a computer with Kaspersky Endpoint Agent installed. The automatic selection of components depends on the permissions of the user account that is upgrading the application.

   If you are upgrading Kaspersky Industrial CyberSecurity for Nodes using the EXE or MSI file under the system account (SYSTEM), Kaspersky Industrial CyberSecurity for Nodes gains access to current licenses of Kaspersky solutions. Therefore, if the computer has, for example, Kaspersky Endpoint Agent installed and the EDR Optimum solution activated, the Kaspersky Industrial CyberSecurity for Nodes installer automatically configures the set of components and selects the EDR Optimum component. This makes Kaspersky Industrial CyberSecurity for Nodes switch to using the built-in agent and removes Kaspersky Endpoint Agent. Running the MSI installer under the system account (SYSTEM) is usually performed when upgrading via the Kaspersky update service (SMU) or when deploying an installation package via Kaspersky Security Center.

   If you are upgrading Kaspersky Industrial CyberSecurity for Nodes using an MSI file under a non-privileged user account, Kaspersky Industrial CyberSecurity for Nodes lacks access to current licenses of Kaspersky solutions. In this case, Kaspersky Industrial CyberSecurity for Nodes automatically selects components based on Kaspersky Endpoint Agent configuration. After that Kaspersky Industrial CyberSecurity for Nodes switches to using the built-in agent and removes Kaspersky Endpoint Agent.

3. **Licensing functionality**

   If you use a common Kaspersky Endpoint Detection and Response Optimum license to activate Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent, EDR Optimum functionality will be activated automatically after upgrading the application to version 5.0. You do not need to do anything else.

   If you use a stand-alone Kaspersky EDR Optimum Add-on license to activate EDR Optimum functionality, you must make sure that the EDR Optimum Add-on key is added to the Kaspersky Security Center repository and the automatic license key distribution functionality is enabled. After you upgrade the application to version 5.0, EDR Optimum functionality is activated automatically.

   If you use a Kaspersky Endpoint Detection and Response Optimum license to activate Kaspersky Endpoint Agent, and a different license to activate Kaspersky Industrial CyberSecurity for Nodes, you must replace the Kaspersky Industrial CyberSecurity for Nodes key with the common Kaspersky Endpoint Detection and Response Optimum key. You can replace the key using the *Add key* task.

4. **Upgrading the Kaspersky Industrial CyberSecurity for Nodes Web Plug-in**

   In the Kaspersky Security Center Web Console, upgrade the Kaspersky Industrial CyberSecurity for Nodes web plug-in to version 5.0.

5. **Migrating the policy and tasks**

   Use the Policy and Task Migration Wizard to migrate Kaspersky Endpoint Agent settings to Kaspersky Industrial CyberSecurity for Nodes.

Migrating the policies and tasks of the [KICS+KEA] configuration to the [KICS+built-in agent] configuration

You can use the Policies and Tasks Migration Wizard of Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent 4.0 or earlier to Kaspersky Industrial CyberSecurity for Nodes 5.0 with built-in agent to migrate policy and task settings for the following solutions:

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR).

The Policies and Tasks Migration Wizard is available only in the Web Console and Cloud Console.

We recommend to begin with migrating policies and tasks of the [KICS+KEA] configuration to [KICS+built-in agent] on a single computer, then do it on a group of computers, and then complete the migration on all computers of the organization.

To migrate the policies and tasks of the [KICS+KEA] configuration to the [KICS+built-in agent] configuration:

In the main window of the Web Console or Cloud Console select **Operations → Migration to Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.

This runs the policies and tasks migration wizard. Follow the instructions of the Wizard.

Step 1. Policy migration

Select Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent policies whose settings you want to merge.

Make sure you selected the correct policies and go to the next step.

Step 2. Task migration

In the task list, select the Kaspersky Industrial CyberSecurity for Nodes tasks that you want to create for Kaspersky Industrial CyberSecurity for Nodes 5.0.

Go to the next step.

Step 3. Wizard completion

Finish the wizard. As a result, the wizard does the following:

- New policies for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  These policies combine settings from previous versions of Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Endpoint Agent. The names of the new policies are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes policies before the merge, with the "copied from KICS" phrase added. New policies has the *Inactive* status. To apply the new merged policy, make it active.

  When migrating from Kaspersky Endpoint Agent to Kaspersky Industrial CyberSecurity for Nodes for the Kaspersky Anti Targeted Attack Platform (EDR) solution, you may encounter errors when connecting the computer to KATA servers. The reason is that the migration wizard skips the following policy settings and does not migrate them:

  - Connection settings modification prohibition ("lock").

    By default, modifying settings is allowed (the "padlock" is open). Therefore the settings are not applied on the computer. You must prohibit the modification of settings and close the "padlock".

  - Crypto-container.

    If you are using two-way authentication for connecting to KATA servers, you must re-add the crypto-container. The migration wizard correctly migrates the TLS certificate of the server.

- New tasks for Kaspersky Industrial CyberSecurity for Nodes 5.0 are created.

  New tasks contain settings from migrated Kaspersky Industrial CyberSecurity for Nodes tasks and also new settings that were introduced in Kaspersky Industrial CyberSecurity for Nodes 5.0. The names of the new tasks are the same as the names of the Kaspersky Industrial CyberSecurity for Nodes tasks before the migration, with the "copied from KICS" phrase added.

SIEM Integration

Kaspersky Industrial CyberSecurity for Nodes allows connecting to SIEM systems to send events for the purposes of analysis and response to potential threats. A SIEM system allows you to detect, analyze, and eliminate security threats before they harm an organization.

SIEM Integration implies that Kaspersky Industrial CyberSecurity for Nodes installed on protected devices running Windows operating systems can send the following Kaspersky Industrial CyberSecurity for Nodes events to the SIEM server:

- Security events. Event conversion to JSON Lines and Syslog (RFC 5424) formats is supported. You can select the events that the application will send to the SIEM server.
- Windows Event Log events. The application converts Windows Event Log events to JSON Lines format. If necessary, you can exclude events from the sent telemetry using filtering rules.

  Kaspersky Industrial CyberSecurity for Nodes, when installed on protected devices running Windows XP, does not support sending Windows Event Log events.

Kaspersky Industrial CyberSecurity for Nodes supports the following protocols for sending events to the SIEM servers:

- TCP
- UDP
- HTTP/HTTPS (for sending Windows Event Log events only)

Setting up SIEM Integration involves the following steps:

1. **Installing the SIEM Integration component**

   In installation package settings or in the Setup Wizard, or by changing the set of application components in the Windows Control Panel, at the step when you must select application components for installation, select the following: **Full functionality** → **Endpoint Agent** → **SIEM Integration**.

2. **Enabling and configuring the SIEM Integration component**

   By default, SIEM integration is not used. You can enable and disable SIEM integration, and configure relevant settings.

   You can reduce the risk of events failing to be sent to the SIEM server by configuring connections to multiple SIEM servers. Kaspersky Industrial CyberSecurity for Nodes connects to the first SIEM server in the list. If a connection attempt fails, Kaspersky Industrial CyberSecurity for Nodes attempts to connect to other servers from the list, one by one. Kaspersky Industrial CyberSecurity for Nodes also uses system audit events to notify you about unsuccessful attempts to connect to the SIEM server and about errors while sending events to the SIEM server.

   How to configure SIEM integration in the Kaspersky Security Center Administration Console

   1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
   2. Select the necessary policy and double-click to open the policy properties.
   3. Select the **Telemetry collection servers** section.

4. In the **SIEM Integration** block, click the **Settings** button.

   The **SIEM Integration** window opens.

5. Select the **SIEM Integration** check box.

6. Configure the SIEM server connection to send security events:

   a. Go to the **Security events transmission settings** tab.

   b. Click **Add**.

   c. This opens the **Add server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

   d. Click **TCP connection security settings**.

   e. This opens the **TCP connection security settings** window; in that window, manage the SIEM server connection settings (see the table below).

   f. If necessary, select the **Remove local copies for events that have been sent to a remote syslog server** check box in the **Settings for event transmission to a SIEM server** block. If the check box is selected, the application deletes the local copies of events after they have been successfully published to the SIEM server. This mode is recommended on low-performance devices. If the check box is cleared, the application only sends events to the SIEM server. Copies of logs continue to be stored locally. By default, the check box is cleared.

      The application never deletes local versions of the security log.

   g. In the **Events format** block, select the format to which you want to convert application events so that they can be sent to the SIEM server:

      - **Convert events to STRUCTURED-DATA** (default value). The application sends events in the Syslog format (RFC 5424).
      - **Convert events to JSON**. The application sends events in the JSON Lines format.

      We recommend that you select the format of events based on the configuration of the utilized SIEM server.

7. Configure the SIEM server connection to send Windows Event Log events:

   a. Go to the **Windows events transmission settings** tab.

   b. If you need to enable the encryption of the connection between Kaspersky Industrial CyberSecurity for Nodes and SIEM servers, under **Settings for connecting to SIEM servers**, select the **Use TLS encryption** check box.

   c. Click **Add**.

   d. This opens the **SIEM server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

   e. Click **Settings for connecting to SIEM servers**.

f. This opens the **Settings for connecting to SIEM servers** window; in that window, manage the SIEM server connection settings (see the table below).

g. If necessary, configure the **Maximum event transmission delay (sec)** setting in the **Data transmission settings** block. When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.

The application sends Windows Event Log events to the SIEM in the JSON Lines format.

8. Close the padlock to apply the policy to computers.

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

How to configure SIEM integration in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Telemetry collection servers** section.

5. In the **SIEM Integration** block, click the **Configure** button.

The **SIEM Integration** window opens.

6. Select the **Enable SIEM Integration** check box.

7. Configure the SIEM server connection to send security events:

a. Go to the **Security events transmission settings** tab.

b. Click **Add**.

c. This opens the **SIEM server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

d. In the **Connection protection** block, click the **Settings for connecting to SIEM servers** link.

e. This opens the **Settings for connecting to SIEM servers** window; in that window, manage the SIEM server connection settings (see the table below).

f. In the **Events format** section, specify the format to which you want to convert application events so that they can be sent to the SIEM server:

- **Convert events to STRUCTURED-DATA** (default value). The application sends events in the Syslog format (RFC 5424).

- **Convert events to JSON**. The application sends events in the JSON Lines format.

We recommend that you select the format of events based on the configuration of the utilized SIEM server.

g. If necessary, select the **Remove local copies for events that have been sent to a remote syslog server** check box in the **Connection settings** block. If the check box is selected, the application deletes the local copies of events after they have been successfully published to the SIEM server. This mode is recommended on low-performance devices. If the check box is cleared, the application only sends events to the SIEM server. Copies of logs continue to be stored locally. By default, the check box is cleared.

> The application never deletes local versions of the security log.

8. Configure the SIEM server connection to send Windows Event Log events:

   a. Go to the **Windows events transmission settings** tab.

   b. Click **Add**.

   c. This opens the **SIEM server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

   d. In the **Connection protection** block, click the **Settings for connecting to SIEM servers** link.

   e. This opens the **Settings for connecting to SIEM servers** window; in that window, manage the SIEM server connection settings (see the table below).

   f. If necessary, configure the **Maximum event transmission delay (sec)** setting in the **Connection settings** block. When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.

   The application sends Windows Event Log events to the SIEM in the JSON Lines format.

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

How to configure SIEM integration in the Application Console

1. In the Application Console tree, select the **Endpoint Agent telemetry → SIEM Integration** section.

2. Click the **Properties** link in the results pane.

   The **Properties: SIEM Integration** window opens.

3. Select the **SIEM Integration** check box.

4. Configure the SIEM server connection to send security events:

   a. Go to the **Security events transmission settings** tab.

   b. Click **Add**.

   c. This opens the **Add server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

   d. Click **TCP connection security settings**.

   e. This opens the **TCP connection security settings** window; in that window, manage the SIEM server connection settings (see the table below).

f. If necessary, select the **Remove local copies for events that have been sent to a remote syslog server** check box in the **Settings for event transmission to a SIEM server** block. If the check box is selected, the application deletes the local copies of events after they have been successfully published to the SIEM server. This mode is recommended on low-performance devices. If the check box is cleared, the application only sends events to the SIEM server. Copies of logs continue to be stored locally. By default, the check box is cleared.

The application never deletes local versions of the security log.

g. In the **Events format** block, select the format to which you want to convert application events so that they can be sent to the SIEM server:

- **Convert events to STRUCTURED-DATA** (default value). The application sends events in the Syslog format (RFC 5424).
- **Convert events to JSON**. The application sends events in the JSON Lines format.

We recommend that you select the format of events based on the configuration of the utilized SIEM server.

5. Configure the SIEM server connection to send Windows Event Log events:

a. Go to the **Windows events transmission settings** tab.

b. If you need to enable the encryption of the connection between Kaspersky Industrial CyberSecurity for Nodes and SIEM servers, under **Settings for connecting to SIEM servers**, select the **Use TLS encryption** check box.

c. Click **Add**.

d. This opens the **SIEM server** window; in that window, enter the SIEM server address (IPv4, DNS), port, and connection protocol.

e. Click **Settings for connecting to SIEM servers**.

f. This opens the **Settings for connecting to SIEM servers** window; in that window, manage the SIEM server connection settings (see the table below).

g. If necessary, configure the **Maximum event transmission delay (sec)** setting in the **Data transmission settings** block. When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. The default setting is 30 seconds.

The application sends Windows Event Log events to the SIEM in the JSON Lines format.

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

SIEM server connection settings

Parameter	Description
Timeout (sec)	Maximum SIEM server response timeout. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes tries to connect to a different SIEM server.

Server TLS certificate	TLS certificate for establishing a trusted connection with the SIEM server. You can get a TLS certificate using the SIEM management interface.
Use two-way authentication	Two-way authentication when establishing a secure connection between Kaspersky Industrial CyberSecurity for Nodes and SIEM. To use two-way authentication, you need to enable two-way authentication in the SIEM settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. After configuring SIEM settings, you need to enable two-way authentication in Kaspersky Industrial CyberSecurity for Nodes settings using a check box and load a password-protected crypto-container. The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

Filtering events to be sent to SIEM

To improve performance and optimize data transmission to the SIEM server, you can manually add or exclude individual Windows Event Log events from telemetry. For example you can exclude Sysmon events.

For the SIEM Integration component to work correctly, enable sending of the required events. By default, sending of all events is disabled.

Kaspersky Industrial CyberSecurity for Nodes supports up to 1500 inclusion and exclusion rules for filtering WEL events for SIEM telemetry.

How to create a list of events to be sent to your SIEM in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Supplementary** section.
4. In the **SIEM telemetry settings** block, click the **Settings** button.
5. In the window that is displayed, configure the event filter to be sent to SIEM.

   You can configure event filtering for the standard *Application*, *Security*, *System* logs or manually add another log:

   a. Open the log properties or click the **Add** button and enter the log name.

   b. Select an event sending mode:

   - **Send all events**. In this mode, the application sends all events from the Windows log except events added to exclusion rules.
   - **Send only selected events**. In this mode, the application sends only events added in inclusion rules.

c. Create lists of exclusion rules or inclusion rules for the relevant event sending mode.

To add rules, you need to specify the ID of the event in the Windows event log. You can list multiple event IDs in a rule. To specify multiple event IDs, use the comma character (,).

d. If necessary, enable event logging using the check box next to the log name.

6. Save your changes. To apply the policy on computers, close the padlocks.

How to create a list of events to be sent to SIEM in Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Supplementary** section.
5. In the **Telemetry settings** block, click the **Configure** button.

   The **Telemetry settings** window opens.
6. Go to the **SIEM telemetry** tab.
7. Configure the event filter for sending to SIEM.

   You can configure event filtering for the standard *Application*, *Security*, *System* logs or manually add another log:

   a. Open the log properties or click the **Add** button and enter the log name.

   b. Select an event sending mode:

   - **Send all events**. In this mode, the application sends all events from the Windows log except events added to exclusion rules.
   - **Send only selected events**. In this mode, the application sends only events added in inclusion rules.

   c. Create lists of exclusion rules or inclusion rules for the relevant event sending mode.

   To add rules, you need to specify the ID of the event in the Windows event log. You can list multiple event IDs in a rule. To specify multiple event IDs, use the comma character (,).

   d. If necessary, enable event logging using the toggle switch next to the log name.
8. Save your changes. To apply the policy on computers, close the padlocks.

Exporting and importing telemetry event filtering rules

Kaspersky Industrial CyberSecurity for Nodes allows importing and exporting JSON files with telemetry event filtering rules.

Kaspersky Industrial CyberSecurity for Nodes supports up to 1500 inclusion and exclusion rules for filtering WEL events for SIEM telemetry.

If event filtering rules already exist on the computer, Kaspersky Industrial CyberSecurity for Nodes replaces these when importing.

Example: You can export the list of exclusions to a JSON file. Then you can modify the file to, for example, add a large number of event IDs. You can also use the export and import function to back up the event filters or to migrate the list to a different server.

How to export and import event filtering rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Supplementary** section.
4. In the **SIEM telemetry** block, click the **Settings** button.
5. To export the event filters:
   a. Select event logs with filters that you want to export.
   b. Click the button to open a context menu and select **Export**.
   c. This opens a window; in that window, specify the name of file to which you want to export the event filters, and select the folder in which you want to save this file.
   d. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the event filters to the JSON file.
6. To import the event filters:
   a. Click the button to open a context menu and select **Import**.
   b. In the window that opens, select the JSON file from which you want to import the event filters.
   c. Open the file.
7. Save your changes. To apply the policy on computers, close the lock .

How to export and import event filtering rules in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Supplementary** section.
5. In the **Telemetry settings** block, click the **Configure** button.

   The **Telemetry settings** window opens.
6. Go to the **SIEM telemetry** tab.
7. To export the event filters:

   a. Select event logs with filters that you want to export.

   b. Click **Export**.

   c. This opens a window; in that window, specify the name of file to which you want to export the event filters, and select the folder in which you want to save this file.

   d. Save the file.

   Kaspersky Industrial CyberSecurity for Nodes exports the event filters to the JSON file.
8. To import the event filters:

   a. Click **Import**.

   b. In the window that opens, select the JSON file from which you want to import the event filters.

   c. Open the file.
9. Save your changes. To apply the policy on computers, close the padlocks.

How to export or import event filtering rules in the Kaspersky Industrial CyberSecurity for Nodes Application Console.

1. In the Application Console tree, select the **Telemetry settings** node.
2. In the **SIEM telemetry** block, click the **Settings** button.
3. To export the event filters:

   a. Click **Export**.

   b. In the window that opens, specify the name of the JSON file to which you want to export the event filters, and select the folder in which you want to save this file.

   c. Save the file.

Kaspersky Industrial CyberSecurity for Nodes exports the event filters to the JSON file.

4. To import the event filters:

   a. Click **Import**.

   b. In the displayed dialog box, confirm the modification of SIEM telemetry settings.

   c. Select the JSON file from which you want to import the event filters.

   d. Open the file.

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

You can also export or import telemetry event filtering rules using the command line interface.

Anomaly Detection using Sigma rules

This functionality is available on computers running Windows 7 or later or Windows Server 2008 R2 or later, if there is an active Kaspersky Industrial CyberSecurity for Nodes license key with the EDR Optimum and ICS Telemetry licensed objects.

For anomaly detection using Sigma rules, you must enable the following components: Real-Time File Protection, Exploit Prevention, Remediation Engine.

Sigma is a format for describing anomaly detection rules that Kaspersky Industrial CyberSecurity for Nodes uses to analyze data from internal events and event logs. Rules written in Sigma format are called Sigma rules.

Sigma rules are written in YAML and have a unified structure. This allows specially created converters to generate rules in the syntax of various SIEM systems based on Sigma rules. Each Sigma rule is stored in a separate YAML file.

Sigma rule structure

The table contains basic information about the attributes and sections of a Sigma rule, which are interpreted by Kaspersky Industrial CyberSecurity for Nodes. For more detailed information, follow this link.

Attribute values are case-sensitive. For example, Kaspersky Industrial CyberSecurity for Nodes treats the names of the executable files AnyDesk.exe and anyDesk.exe as different.

<table>
<tr><th>Attribute / Section</th><th>Required</th><th>Description</th></tr>
<tr><td><code>logsource</code></td><td>Yes</td><td>
In this section, you can define the source of events that the application will search for anomalies. The main attributes of this section are <code>category</code>, <code>product</code>, and <code>service</code>.
Event sources that Kaspersky Industrial CyberSecurity for Nodes supports
Event sources supported by Kaspersky Industrial CyberSecurity for Nodes
<table>
<tr><th>Source (logsource)</th><th>Event</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal process startup event that corresponds in content to EventID 1 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal driver load event that corresponds in content to EventID 6 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 7 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events that correspond in content to the events EventID 12, EventID 13, and EventID 14 in the Microsoft-Windows-Sysmon/Operational log and are enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 22 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to an event in the log of the Windows trace service provider Microsoft-Windows-Kernel-File and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 11 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Application log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Security log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/System log.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events associated with normalized data from the event logs of the Emerson DeltaV system.
Source events are not linked to external event logs.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Windows PowerShell log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Microsoft-Windows-PowerShell/Operational log.</td></tr>
</table>
In Microsoft Windows 7, for <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> providers, you some internal events are missing, or some fields or necessary data may be missing in events. As a result, Sigma rules may not trigger.
Read more at this link.
</td></tr>
<tr><td><code>title</code></td><td>Yes</td><td>The rule name, which indicates what it detects. The maximum length is 256 characters.
For example:
<code>title: Creation of a new RAT service</code></td></tr>
<tr><td><code>id</code></td><td>No</td><td>The rule's globally unique identifier. For example:
<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code></td></tr>
<tr><td><code>status</code></td><td>No</td><td>Rule status. Possible values: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.
For example:
<code>status: test</code></td></tr>
<tr><td><code>description</code></td><td>No</td><td>A description of the rule and the malicious activity it can detect. The maximum length is 65,535 characters.
For example:
<code>description: Detects the installation of a new Remote Utilities host application service.</code></td></tr>
</table>

`license`	No	License ID according to the SPDX ID specification. The rule is published under the terms of the specified license type.
`author`	No	Any specifier that indicates the author of the rule. For example, first name and last name, nickname, social network ID.
`reference`	No	Link to the source the rule was taken from. For example, a blog article or white paper.
`date`	No	Date when the rule was created in YYYY/MM/DD format.
`modified`	No	Date in YYYY/MM/DD format when one of the following rule attributes was changed: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	No	Tag for categorizing the rule. Read more at this link.

`category`	No	Defines the category of products whose event logs the application searches for anomalies. For example: firewall, internet, anti-virus, or generic.
		`logsource:`
		`  category: firewall`

`product`	No	Defines the software product or operating system whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  product: Windows`

`service`	No	Defines a service whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  service: AppLocker`

`definition`	No	Description of the specifics of the source of event logs that application searches for anomalies.
`detection`	Yes	This section contains one or more criteria for searching for anomalies in event logs and a rule triggering condition. Lists, dictionaries, or a combination of them can be used as search criteria. Kaspersky Industrial CyberSecurity for Nodes does not support the `windash` value modifier.

list	No	A list of the values of any parameter from the event log, combined by a logical OR. For example:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: `OriginalFileName='AnyDesk.exe'` OR `OriginalFileName='TeamViewer.exe'`.

dictionary	No	*event log parameter* - *value* pairs. They are connected by a logical AND. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND Event ID=517.

combination of list and dictionary	No	A list consisting of event log settings values and dictionaries. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	Yes	Rule-triggering condition. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	No	Lines from the event log that may be of interest to an analyst for subsequent analysis of the event.

`falsepositives`	No	List of known scenarios that may incorrectly trigger the rule. For example:
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	No	An indicator of the severity of anomalies that can be found using the rule. Possible values: `informational`, `low`, `medium`, `high`, `critical`.

Example of a Sigma rule

```
title: Downloading files using CertUtil.exe
id: 89346938-3b2f-46c7-bb38-b9f244e3fad0
status: test
description: Detects file downloads using CertUtil.exe.
references:
  - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
author: Kaspersky
date: 2024-05-22
tags:
  - attack.defense_evasion
  - attack.t1027
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    - Image|endswith: '\certutil.exe'
    - OriginalFileName: 'CertUtil.exe'
  selection_http:
    CommandLine|contains: 'http'
condition: all of selection_*
falsepositives:
  - Legitimate actions of the system administrator.
level: low
```

A *collection of Sigma rules* is a set of Sigma rules that define similar events.

Kaspersky Industrial CyberSecurity for Nodes analyzes data from internal events and event logs to find anomalies using collections of Kaspersky-supplied Sigma rules and the application databases, and using collections of Sigma rules created by the user.

Depending on the version of the application, Kaspersky Industrial CyberSecurity for Nodes supports working with predefined collections of Sigma rules, which are listed in the table below.

Predefined Sigma rules collections

Sigma rules collection	Application version	
	4.5	5.0
Detection of remote administration tools (RAT)	✓	✓
Anomaly detection for Emerson DeltaV	✓	✓
User account control (UAC)	✓	✓
Anomaly detection for Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7	✓	✓
Anomaly detection for Yokogawa CENTUM VP	✓	✓
Audit of file sharing over a network and via removable media	–	✓

When using some Sigma rules, the application can make changes to the security audit policy of the protected computer - part of the local Windows security policy.

Special considerations and limitations of Anomaly Detection using Sigma Rules

For some collections of Sigma rules to work correctly, audit policy settings need to be modified. The behavior of the application depends on whether the computer belongs to a domain or not:

- If the computer belongs to a domain, the application does not modify domain group policy settings. You can exclude such a computer from the domain or configure domain group policy settings manually.
- If the computer does not belong to a domain, the application automatically edits local policy settings if this is necessary for the collection of Sigma rules to work correctly.

  To have local policy settings modified automatically, the Automatically make changes to the local security audit policy functionality must be enabled. If it is disabled, take steps to manually configure local policy settings for the Sigma rules to work correctly.

  The application does not modify the local policy settings for custom collections of Sigma rules. You need to manually configure local policy settings for the custom Sigma rules to work correctly.

  After the collection of Sigma rules is disabled, the application does not revert local policy settings to their original values. If necessary, you can manually restore the original local policy settings.

The Anomaly Detection using Sigma rules functionality has the following limitations:

- For the "Windows Event Log modification or deletion on DeltaV host" Sigma rule to work, immediately after installing the "Anomaly Detection using Sigma rules" component, you must restart the computer or **stop the Windows Event Log service and start it again**.

  1. Start the Windows Services application (services.msc).
  2. In the list of services, find Windows Event Log.
  3. In the context menu of the Windows Event Log service, select **Stop** to stop the service.
  4. In the context menu of the Windows Event Log service, select **Start** to start the service.

- The following value modifiers are not supported: `base64offset`, `cidr`, `lt`, `windash`.
- Regular expressions are not supported.
- Escaping of wildcard characters is not supported.
- The application treats the `?` wildcard as `*`.
- The "`condition: not selection`" construct is not supported; however, the "`condition: selection and not filter`" construct is supported.

- Rules that do not have one or more values of the `EventID` parameter specified as criteria for searching Windows event logs for anomalies are not supported.
- For Sigma rules that describe file operations, the report includes the first 50 detections. If a process performs operations on files that have similar paths, detections are counted separately for each process.
- The application supports Sigma rules on Windows XP and Windows Server 2003 computers with some limitations. Opening alert details for detections on computers running these operating systems may fail with the *Failed to open the alert details. Possible reasons: host is offline, problems with the network, alert storage time has expired* error. You can open alert details using Kaspersky Industrial CyberSecurity for Networks.
- The application supports integration with Siemens SIMATIC PCS 7 version 9.0 SP1 or later.
- To ensure the "Removable drive file writing detection" Sigma rule from the Audit of file sharing over a network and via removable media predefined collection works properly, a computer restart is required.

Enabling Anomaly Detection using Sigma Rules

Enabling Anomaly Detection using Sigma Rules in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Anomaly Detection using Sigma rules** section.
4. In the **Anomaly Detection using Sigma rules** block, click the **Settings** button.
5. In the window that opens, select the **Anomaly Detection using Sigma rules** check box.
6. Add one or more collections of Sigma rules:

   a. Click **Add**.

   The **Add rules collection** window opens.

   b. Use the **Choose a rules collection** drop-down list to do one of the following:

   - Select one of the predefined Sigma rule collections.

     If predefined Sigma rule collections are not displayed, make sure the application is activated with a license key with EDR Optimum and ICS Telemetry objects. You can also run the *Download updates to the Administration Server repository* task to update predefined collections.

     When adding predefined collections of Sigma rules, you need to make sure that the selected collection is supported by all versions of Kaspersky Industrial CyberSecurity for Nodes installed on managed devices.

   - Select the **Custom rules collection** option to add a custom collection of Sigma rules.

     If you are adding a custom collection of Sigma rules, enter a unique name for the collection in the corresponding field. The created custom collection does not contain any rules.

c. Click **OK**.

The added collection will be displayed in the list. By default, an added collection of Sigma rules is enabled. If necessary, manage the state of the collection of Sigma rules using the check box to the left of the collection name.

7. If necessary, clear the **Automatically make changes to the local security audit policy** check box. If this functionality is enabled, the application automatically edits local policy settings if this is necessary for the added collections of Sigma rules to work correctly. If it is disabled, take steps to manually configure local policy settings for the Sigma rules to work correctly. This option is enabled by default.

> The application does not modify the local policy settings for custom collections of Sigma rules. You need to manually configure local policy settings for the custom Sigma rules to work correctly.

8. Close the padlock to apply the policy to computers.

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

Kaspersky Industrial CyberSecurity for Nodes will search for anomalies using the enabled collections of Sigma rules.

Enabling Anomaly Detection using Sigma Rules in the Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

The policy properties window opens.

3. Select the **Application settings** tab.

4. In the **Anomaly Detection using Sigma rules** section, select the **Enable Anomaly Detection using Sigma rules** check box.

5. If necessary, clear the **Automatically make changes to the local security audit policy** check box. If this functionality is enabled, the application automatically edits local policy settings if this is necessary for the added collections of Sigma rules to work correctly. If it is disabled, take steps to manually configure local policy settings for the Sigma rules to work correctly. This option is enabled by default.

> The application does not modify the local policy settings for custom collections of Sigma rules. You need to manually configure local policy settings for the custom Sigma rules to work correctly.

6. Add one or more collections of Sigma rules:

a. Click **Add**.

The **Add rules collection** window opens.

b. Use the **Choose a rules collection** drop-down list to do one of the following:

- Select one of the predefined Sigma rule collections.

  If predefined Sigma rule collections are not displayed, make sure the application is activated with a license key with EDR Optimum and ICS Telemetry objects. You can also run the *Download updates to the Administration Server repository* task to update predefined collections.

When adding predefined collections of Sigma rules, you need to make sure that the selected collection is supported by all versions of Kaspersky Industrial CyberSecurity for Nodes installed on managed devices.

- Select the **Custom rules collection** option to add a custom collection of Sigma rules.

  If you are adding a custom collection of Sigma rules, enter a unique name for the collection in the corresponding field. The created custom collection does not contain any rules.

c. Click **OK**.

The added collection will be displayed in the list. By default, an added collection of Sigma rules is enabled. If necessary, manage the state of the collection of Sigma rules using the toggle switch to the left of the collection name.

d. Click **Save**.

Kaspersky Industrial CyberSecurity for Nodes will search for anomalies using the enabled collections of Sigma rules.

Enabling Anomaly Detection using Sigma Rules in the Application Console

1. In the Application Console tree, select the **Detection and Response → Anomaly Detection using Sigma rules** section.

   Click the **Properties** link in the results pane.

2. Select the **Anomaly Detection using Sigma rules** check box.

3. Add one or more collections of Sigma rules:

   a. Click **Add**.

   The **Add rules collection** window opens.

   b. Use the **Choose a rules collection** drop-down list to do one of the following:

   - Select one of the predefined Sigma rule collections.

     If predefined Sigma rule collections are not displayed, make sure the application is activated with a license key with EDR Optimum and ICS Telemetry objects. You can also run the *Download updates to the Administration Server repository* task to update predefined collections.

   - Select the **Custom rules collection** option to add a custom collection of Sigma rules.

     If you are adding a custom collection of Sigma rules, enter a unique name for the collection in the corresponding field. The created custom collection does not contain any rules.

     Custom collections of Sigma rules created using the Application Console are not available in the Kaspersky Security Center Administration Console and Web Console.

   c. Click **OK**.

   The added collection will be displayed in the list. By default, an added collection of Sigma rules is enabled. If necessary, manage the state of the collection of Sigma rules using the check box to the left of the collection name.

4. If necessary, clear the **Automatically make changes to the local security audit policy** check box. If this functionality is enabled, the application automatically edits local policy settings if this is necessary for the added collections of Sigma rules to work correctly. If it is disabled, take steps to manually configure local policy settings for the Sigma rules to work correctly. This option is enabled by default.

   The application does not modify the local policy settings for custom collections of Sigma rules. You need to manually configure local policy settings for the custom Sigma rules to work correctly.

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

   Kaspersky Industrial CyberSecurity for Nodes will search for anomalies using the enabled collections of Sigma rules.

You can also enable Anomaly Detection using Sigma rules on the command line.

Adding Sigma rules to a custom collection

Adding Sigma rules to a custom collection in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Anomaly Detection using Sigma rules** section.
4. In the **Anomaly Detection using Sigma rules** block, click the **Settings** button.
5. In the window that opens, select a custom Sigma rule collection to which you want to add one or more Sigma rules.
6. Click **Edit**.
7. In the window that opens, add a Sigma rule to the collection in any of the following ways:

   - Manually:

     a. Click **Add**.

     b. In the editor form that opens, describe the rule **in Sigma format**.

     The table contains basic information about the attributes and sections of a Sigma rule, which are interpreted by Kaspersky Industrial CyberSecurity for Nodes. For more detailed information, follow this link.

     Attribute values are case-sensitive. For example, Kaspersky Industrial CyberSecurity for Nodes treats the names of the executable files AnyDesk.exe and anyDesk.exe as different.

<table>
<tr><th>Attribute / Section</th><th>Required</th><th>Description</th></tr>
<tr><td><code>logsource</code></td><td>Yes</td><td>
In this section, you can define the source of events that the application will search for anomalies. The main attributes of this section are <code>category</code>, <code>product</code>, and <code>service</code>.

Event sources that Kaspersky Industrial CyberSecurity for Nodes supports

Event sources supported by Kaspersky Industrial CyberSecurity for Nodes

<table>
<tr><th>Source (logsource)</th><th>Event</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal process startup event that corresponds in content to EventID 1 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal driver load event that corresponds in content to EventID 6 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 7 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events that correspond in content to the events EventID 12, EventID 13, and EventID 14 in the Microsoft-Windows-Sysmon/Operational log and are enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 22 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to an event in the log of the Windows trace service provider Microsoft-Windows-Kernel-File and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 11 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Application log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Security log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/System log.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events associated with normalized data from the event logs of the Emerson DeltaV system.
Source events are not linked to external event logs.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Windows PowerShell log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Microsoft-Windows-PowerShell/Operational log.</td></tr>
</table>

In Microsoft Windows 7, for <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> providers, you some internal events are missing, or some fields or necessary data may be missing in events. As a result, Sigma rules may not trigger.

Read more at this link.
</td></tr>
<tr><td><code>title</code></td><td>Yes</td><td>
The rule name, which indicates what it detects. The maximum length is 256 characters.

For example:

<code>title: Creation of a new RAT service</code>
</td></tr>
<tr><td><code>id</code></td><td>No</td><td>
The rule's globally unique identifier. For example:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code>
</td></tr>
<tr><td><code>status</code></td><td>No</td><td>
Rule status. Possible values: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

For example:

<code>status: test</code>
</td></tr>
</table>

`description`	No	A description of the rule and the malicious activity it can detect. The maximum length is 65,535 characters. For example: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	No	License ID according to the SPDX ID specification. The rule is published under the terms of the specified license type.
`author`	No	Any specifier that indicates the author of the rule. For example, first name and last name, nickname, social network ID.
`reference`	No	Link to the source the rule was taken from. For example, a blog article or white paper.
`date`	No	Date when the rule was created in YYYY/MM/DD format.
`modified`	No	Date in YYYY/MM/DD format when one of the following rule attributes was changed: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	No	Tag for categorizing the rule. Read more at this link.

`category`	No	Defines the category of products whose event logs the application searches for anomalies. For example: firewall, internet, anti-virus, or generic.
		`logsource:`
		`  category: firewall`

`product`	No	Defines the software product or operating system whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  product: Windows`

`service`	No	Defines a service whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  service: AppLocker`

`definition`	No	Description of the specifics of the source of event logs that application searches for anomalies.
`detection`	Yes	This section contains one or more criteria for searching for anomalies in event logs and a rule triggering condition. Lists, dictionaries, or a combination of them can be used as search criteria. Kaspersky Industrial CyberSecurity for Nodes does not support the `windash` value modifier.

list	No	A list of the values of any parameter from the event log, combined by a logical OR. For example:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: `OriginalFileName='AnyDesk.exe'` OR `OriginalFileName='TeamViewer.exe'`.

dictionary	No	*event log parameter* - *value* pairs. They are connected by a logical AND. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND Event ID=517.

combination of list and dictionary	No	A list consisting of event log settings values and dictionaries. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	Yes	Rule-triggering condition. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	No	Lines from the event log that may be of interest to an analyst for subsequent analysis of the event.

`falsepositives`	No	List of known scenarios that may incorrectly trigger the rule. For example:
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	No	An indicator of the severity of anomalies that can be found using the rule. Possible values: `informational`, `low`, `medium`, `high`, `critical`.

c. Click **OK**.

The described Sigma rule will be displayed in the list of rules in the collection.

d. Repeat steps a-c for each rule being manually added.

- From files:

a. Click **Add file**.

b. In the window that opens, select one or more YAML files that describe Sigma rules.

Sigma rules described in YAML files will be displayed in the list of rules in the collection.

> If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

8. By default, the added rules are enabled. If necessary, manage the state of a Sigma rule using the check box to the left of the collection name. You can change the state of all rules in the collection using the **Enable all** and **Disable all** buttons.

9. To delete a rule from the list, select the rule and click **Remove**.

10. Save your changes.

Adding Sigma rules to a custom collection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

The policy properties window opens.

3. Select the **Application settings** tab.

4. Select the **Anomaly Detection using Sigma rules** section.

5. In the **Anomaly Detection using Sigma rules** block, using the check box next to the collection name, select a custom Sigma rule collection to which you want to add one or more Sigma rules.

6. Click **Edit**.

7. In the window that opens, add a Sigma rule to the collection in any of the following ways:

- Manually:

  a. Click **Add**.

  b. In the editor form that opens, describe the rule **in Sigma format**.

  The table contains basic information about the attributes and sections of a Sigma rule, which are interpreted by Kaspersky Industrial CyberSecurity for Nodes. For more detailed information, follow this link.

  > Attribute values are case-sensitive. For example, Kaspersky Industrial CyberSecurity for Nodes treats the names of the executable files AnyDesk.exe and anyDesk.exe as different.

<table>
<tr><th>Attribute / Section</th><th>Required</th><th>Description</th></tr>
<tr><td><code>logsource</code></td><td>Yes</td><td>
In this section, you can define the source of events that the application will search for anomalies. The main attributes of this section are <code>category</code>, <code>product</code>, and <code>service</code>.

Event sources that Kaspersky Industrial CyberSecurity for Nodes supports

Event sources supported by Kaspersky Industrial CyberSecurity for Nodes

<table>
<tr><th>Source (logsource)</th><th>Event</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal process startup event that corresponds in content to EventID 1 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal driver load event that corresponds in content to EventID 6 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 7 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events that correspond in content to the events EventID 12, EventID 13, and EventID 14 in the Microsoft-Windows-Sysmon/Operational log and are enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 22 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to an event in the log of the Windows trace service provider Microsoft-Windows-Kernel-File and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 11 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Application log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Security log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/System log.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events associated with normalized data from the event logs of the Emerson DeltaV system.
Source events are not linked to external event logs.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Windows PowerShell log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Microsoft-Windows-PowerShell/Operational log.</td></tr>
</table>

In Microsoft Windows 7, for <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> providers, you some internal events are missing, or some fields or necessary data may be missing in events. As a result, Sigma rules may not trigger.

Read more at this link.
</td></tr>
<tr><td><code>title</code></td><td>Yes</td><td>
The rule name, which indicates what it detects. The maximum length is 256 characters.

For example:

<code>title: Creation of a new RAT service</code>
</td></tr>
<tr><td><code>id</code></td><td>No</td><td>
The rule's globally unique identifier. For example:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code>
</td></tr>
<tr><td><code>status</code></td><td>No</td><td>
Rule status. Possible values: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

For example:

<code>status: test</code>
</td></tr>
</table>

`description`	No	A description of the rule and the malicious activity it can detect. The maximum length is 65,535 characters. For example: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	No	License ID according to the SPDX ID specification. The rule is published under the terms of the specified license type.
`author`	No	Any specifier that indicates the author of the rule. For example, first name and last name, nickname, social network ID.
`reference`	No	Link to the source the rule was taken from. For example, a blog article or white paper.
`date`	No	Date when the rule was created in YYYY/MM/DD format.
`modified`	No	Date in YYYY/MM/DD format when one of the following rule attributes was changed: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	No	Tag for categorizing the rule. Read more at this link.

`category`	No	Defines the category of products whose event logs the application searches for anomalies. For example: firewall, internet, anti-virus, or generic.
		`logsource:`
		`  category: firewall`

`product`	No	Defines the software product or operating system whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  product: Windows`

`service`	No	Defines a service whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  service: AppLocker`

`definition`	No	Description of the specifics of the source of event logs that application searches for anomalies.
`detection`	Yes	This section contains one or more criteria for searching for anomalies in event logs and a rule triggering condition. Lists, dictionaries, or a combination of them can be used as search criteria. Kaspersky Industrial CyberSecurity for Nodes does not support the `windash` value modifier.

list	No	A list of the values of any parameter from the event log, combined by a logical OR. For example:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: `OriginalFileName='AnyDesk.exe'` OR `OriginalFileName='TeamViewer.exe'`.

dictionary	No	*event log parameter* - *value* pairs. They are connected by a logical AND. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND Event ID=517.

combination of list and dictionary	No	A list consisting of event log settings values and dictionaries. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	Yes	Rule-triggering condition. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	No	Lines from the event log that may be of interest to an analyst for subsequent analysis of the event.

`falsepositives`	No	List of known scenarios that may incorrectly trigger the rule. For example:
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	No	An indicator of the severity of anomalies that can be found using the rule. Possible values: `informational`, `low`, `medium`, `high`, `critical`.

c. Click **OK**.

The described Sigma rule will be displayed in the list of rules in the collection.

d. Repeat steps a-c for each rule being manually added.

- From files:

a. Click **Add file**.

b. In the window that opens, select one or more YAML files that describe Sigma rules.

Sigma rules described in YAML files will be displayed in the list of rules in the collection.

> If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

8. By default, the added rules are enabled. If necessary, manage the state of the collection of Sigma rules using the toggle switch to the left of the collection name. You can change the state of all rules in the collection using the **Enable all** and **Disable all** buttons.

9. To delete a rule from the list, select the rule and click **Delete**.

10. Save your changes.

Adding Sigma rules to a custom collection in the Application Console

1. In the Application Console tree, select the **Detection and Response → Anomaly Detection using Sigma rules** section.

2. Click the **Properties** link in the results pane.

3. In the window that opens, select a custom Sigma rule collection to which you want to add one or more Sigma rules.

4. Click **Edit**.

5. In the window that opens, add a Sigma rule to the collection in any of the following ways:

- Manually:

  a. Click **Add**.

  b. In the editor form that opens, describe the rule **in Sigma format**.

  The table contains basic information about the attributes and sections of a Sigma rule, which are interpreted by Kaspersky Industrial CyberSecurity for Nodes. For more detailed information, follow this link.

  > Attribute values are case-sensitive. For example, Kaspersky Industrial CyberSecurity for Nodes treats the names of the executable files AnyDesk.exe and anyDesk.exe as different.

<table>
<tr><th>Attribute / Section</th><th>Required</th><th>Description</th></tr>
<tr><td><code>logsource</code></td><td>Yes</td><td>
In this section, you can define the source of events that the application will search for anomalies. The main attributes of this section are <code>category</code>, <code>product</code>, and <code>service</code>.

Event sources that Kaspersky Industrial CyberSecurity for Nodes supports

Event sources supported by Kaspersky Industrial CyberSecurity for Nodes

<table>
<tr><th>Source (logsource)</th><th>Event</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal process startup event that corresponds in content to EventID 1 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal driver load event that corresponds in content to EventID 6 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 7 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events that correspond in content to the events EventID 12, EventID 13, and EventID 14 in the Microsoft-Windows-Sysmon/Operational log and are enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 22 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to an event in the log of the Windows trace service provider Microsoft-Windows-Kernel-File and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of an internal event that corresponds in content to EventID 11 in the Microsoft-Windows-Sysmon/Operational log and is enriched by Kaspersky Industrial CyberSecurity for Nodes fields.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Application log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/Security log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the WEL/System log.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes instances of internal events associated with normalized data from the event logs of the Emerson DeltaV system.
Source events are not linked to external event logs.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Windows PowerShell log.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes analyzes events from the Microsoft-Windows-PowerShell/Operational log.</td></tr>
</table>

In Microsoft Windows 7, for <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> providers, you some internal events are missing, or some fields or necessary data may be missing in events. As a result, Sigma rules may not trigger.

Read more at this link.
</td></tr>
<tr><td><code>title</code></td><td>Yes</td><td>
The rule name, which indicates what it detects. The maximum length is 256 characters.

For example:

<code>title: Creation of a new RAT service</code>
</td></tr>
<tr><td><code>id</code></td><td>No</td><td>
The rule's globally unique identifier. For example:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code>
</td></tr>
<tr><td><code>status</code></td><td>No</td><td>
Rule status. Possible values: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

For example:

<code>status: test</code>
</td></tr>
</table>

`description`	No	A description of the rule and the malicious activity it can detect. The maximum length is 65,535 characters. For example: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	No	License ID according to the SPDX ID specification. The rule is published under the terms of the specified license type.
`author`	No	Any specifier that indicates the author of the rule. For example, first name and last name, nickname, social network ID.
`reference`	No	Link to the source the rule was taken from. For example, a blog article or white paper.
`date`	No	Date when the rule was created in YYYY/MM/DD format.
`modified`	No	Date in YYYY/MM/DD format when one of the following rule attributes was changed: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	No	Tag for categorizing the rule. Read more at this link.

`category`	No	Defines the category of products whose event logs the application searches for anomalies. For example: firewall, internet, anti-virus, or generic.
		`logsource:`
		`  category: firewall`

`product`	No	Defines the software product or operating system whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  product: Windows`

`service`	No	Defines a service whose event logs the application searches for anomalies. For example:
		`logsource:`
		`  service: AppLocker`

`definition`	No	Description of the specifics of the source of event logs that application searches for anomalies.
`detection`	Yes	This section contains one or more criteria for searching for anomalies in event logs and a rule triggering condition. Lists, dictionaries, or a combination of them can be used as search criteria. Kaspersky Industrial CyberSecurity for Nodes does not support the `windash` value modifier.

list	No	A list of the values of any parameter from the event log, combined by a logical OR. For example:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: `OriginalFileName='AnyDesk.exe'` OR `OriginalFileName='TeamViewer.exe'`.

dictionary	No	*event log parameter* - *value* pairs. They are connected by a logical AND. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND Event ID=517.

combination of list and dictionary	No	A list consisting of event log settings values and dictionaries. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		In accordance with the condition, the following matches will be searched: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	Yes	Rule-triggering condition. For example:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	No	Lines from the event log that may be of interest to an analyst for subsequent analysis of the event.

`falsepositives`	No	List of known scenarios that may incorrectly trigger the rule. For example:
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	No	An indicator of the severity of anomalies that can be found using the rule. Possible values: `informational`, `low`, `medium`, `high`, `critical`.

c. Click **OK**.

The described Sigma rule will be displayed in the list of rules in the collection.

d. Repeat steps a-c for each rule being manually added.

- From files:

a. Click **Add file**.

b. In the window that opens, select one or more YAML files that describe Sigma rules.

Sigma rules described in YAML files will be displayed in the list of rules in the collection.

> If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

6. By default, the added rules are enabled. If necessary, manage the state of a Sigma rule using the check box to the left of the collection name. You can change the state of all rules in the collection using the **Enable all** and **Disable all** buttons.

7. To delete a rule from the list, select the rule and click **Remove**.

8. Save your changes.

Filtering Sigma rules within a collection of rules

If a collection contains a large number of Sigma rules and you need to display a list of Sigma rules with certain parameters, you can use a filter.

Filtering a Sigma rule in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. Select the **Anomaly Detection using Sigma rules** section.

4. In the **Anomaly Detection using Sigma rules** block, click the **Settings** button.

5. In the window that opens, select the collection to which you want to apply the rule filter.

6. Click **Edit**.

The **Edit** window opens.

7. Click **Filter**.

   A window with filtering criteria opens.

8. Specify the values of the filtering criteria you need:

   - The **A rule contains the text** criterion selects rules based on a case-insensitive match of the fragment. You can enter any rule attribute and/or its value.
   - The **Rule state** criterion selects rules based on their state.
   - The **Availability of exclusions** criterion selects rules based on the presence of exclusions.

     This criterion is available only for filtering rules in a collection supplied by Kaspersky.

9. Click **OK**.

   The rules that match the filtering criteria are displayed in the list of rules in the collection.

Filtering a Sigma rule in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.
4. Select the **Anomaly Detection using Sigma rules** section.
5. In the **Anomaly Detection using Sigma rules** block, use the check box to select the collection to which you want to apply the rule filter.
6. Click **Edit**.

   The **Edit** window opens.

7. Click **Filter**.

   A window with filtering criteria opens.

8. Specify the values of the filtering criteria you need:

   - The **A rule contains the text** criterion selects rules based on a case-insensitive match of the fragment. You can enter any rule attribute and/or its value.
   - The **Rule state** criterion selects rules based on their state.
   - The **Availability of exclusions** criterion selects rules based on the presence of exclusions.

     This criterion is available only for filtering rules in a collection supplied by Kaspersky.

9. Click **OK**.
10. The rules that match the filtering criteria are displayed in the list of rules in the collection.

Filtering a Sigma rule in the Application Console

1. In the Application Console tree, select the **Detection and Response → Anomaly Detection using Sigma rules** section.

   Click the **Properties** link in the results pane.

2. In the window that opens, select the collection to which you want to apply the rule filter.

3. Click **Edit**.

   The **Edit** window opens.

4. Click **Filter**.

   A window with filtering criteria opens.

5. Specify the values of the filtering criteria you need:

   - The **A rule contains the text** criterion selects rules based on a case-insensitive match of the fragment. You can enter any rule attribute and/or its value.
   - The **Rule state** criterion selects rules based on their state.
   - The **Availability of exclusions** criterion selects rules based on the presence of exclusions.

     This criterion is available only for filtering rules in a collection supplied by Kaspersky.

6. Click **OK**.

   The rules that match the filtering criteria are displayed in the list of rules in the collection.

Exporting and importing Sigma rules of a custom collection

Exporting and importing Sigma rules in Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. Select the **Anomaly Detection using Sigma rules** section.

4. In the **Anomaly Detection using Sigma rules** block, click the **Settings** button.

5. In the window that opens, select a custom Sigma rule collection.

6. Click **Edit**.

7. Click the **Export** button to export Sigma rules from a custom collection.

   Kaspersky Industrial CyberSecurity for Nodes saves an archive named sigma.zip in the standard download folder.

8. To import Sigma rules into a custom collection:

    a. Click **Import**.

    b. In the window that opens, select the ZIP archive that contains the YAML files with the described Sigma rules.

    > If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

    Sigma rules contained in the archive will be displayed in the list of rules in the collection.

    > If the imported ZIP archive contains duplicate Sigma rules that already exist in the collection, these rules will not be overwritten.

9. Save your changes.

Exporting and importing Sigma rules in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

    The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Anomaly Detection using Sigma rules** section.
5. In the **Anomaly Detection using Sigma rules** block, using the check box next to the collection name, select a custom Sigma rule collection.
6. Click **Edit**.
7. Click the **Export** button to export Sigma rules from a custom collection.

    Kaspersky Industrial CyberSecurity for Nodes saves an archive named sigma.zip in the standard download folder.
8. To import Sigma rules into a custom collection:

    a. Click **Import**.

    b. In the window that opens, select the ZIP archive that contains the YAML files with the described Sigma rules.

    > If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

    Sigma rules contained in the archive will be displayed in the list of rules in the collection.

If the imported ZIP archive contains duplicate Sigma rules that already exist in the collection, these rules will not be overwritten.

9. Save your changes.

Exporting and importing Sigma rules in the Application Console

1. In the Application Console tree, select the **Detection and Response → Anomaly Detection using Sigma rules** section.
2. Click the **Properties** link in the results pane.
3. In the window that opens, select a custom Sigma rule collection.
4. Click **Edit**.
5. Click the **Export** button to export Sigma rules from a custom collection.

   Kaspersky Industrial CyberSecurity for Nodes saves an archive named sigma.zip in the standard download folder.
6. To import Sigma rules into a custom collection:

   a. Click **Import**.

   b. In the window that opens, select the ZIP archive that contains the YAML files with the described Sigma rules.

   If a Sigma rule contains syntax errors or if mandatory attributes are missing, the rule will not be added to the collection.

   Sigma rules contained in the archive will be displayed in the list of rules in the collection.

   If the imported ZIP archive contains duplicate Sigma rules that already exist in the collection, these rules will not be overwritten.
7. Save your changes.

Changing a Sigma rule

You can make any changes to custom Sigma rules. For Sigma rules supplied by Kaspersky Lab as part of predefined collections, only adding or removing exclusions and changing the rule state are allowed.

Changing a Sigma rule in Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. Select the **Anomaly Detection using Sigma rules** section.

4. In the **Anomaly Detection using Sigma rules** block, click the **Settings** button.
5. In the window that opens, select a custom Sigma rule collection in which you want to edit one or more Sigma rules.
6. Click **Edit**.
7. In the window that opens, select the rule that you want to edit.
8. If necessary, change the rule state using the check box to the left of the rule name.
9. Click **Edit**.
10. In the window that opens, make the necessary edits to the Sigma rule.

    If you are editing a Sigma rule supplied by Kaspersky Lab as part of a collection, you are permitted to edit only the exclusions for the rule.

11. Save your changes.

Editing a Sigma rule in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Anomaly Detection using Sigma rules** section.
5. In the **Anomaly Detection using Sigma rules** block, using the check box next to the collection name, select a custom Sigma rule collection in which you want to edit one or more Sigma rules.
6. Click **Edit**.
7. In the window that opens, using the check box, select the rule that you want to edit.
8. If necessary, change the rule state using the **Enabled** / **Disabled** toggle button above the rule name.
9. Click **Edit**.
10. In the window that opens, make the necessary edits to the Sigma rule.

    If you are editing a Sigma rule supplied by Kaspersky Lab as part of a collection, you are permitted to edit only the exclusions for the rule.

11. Save your changes.

Editing a Sigma rule in the Application Console

1. In the Application Console tree, select the **Detection and Response → Anomaly Detection using Sigma rules** section.
2. Click the **Properties** link in the results pane.
3. In the window that opens, select a custom Sigma rule collection in which you want to edit one or more Sigma rules.
4. Click **Edit**.
5. In the window that opens, select the rule that you want to edit.
6. If necessary, change the rule state using the check box to the left of the rule name.
7. Click **Edit**.
8. In the window that opens, make the necessary edits to the Sigma rule.

   If you are editing a Sigma rule supplied by Kaspersky Lab as part of a collection, you are permitted to edit only the exclusions for the rule.

9. Save your changes.

Exclusions in a Sigma rule

The content of Sigma rules supplied with the application databases is unavailable to the user. This is because the triggering conditions for these rules are Kaspersky's intellectual property and cannot be disclosed.

In the editor for editing a Sigma rule supplied with the application databases, you can only add exclusions from the rule in the `detection` section.

The exclusion template is defined as follows:

```
detection:
   exclude1:
        - ...
   condition: not 1 of exclude*
```

This template assumes that exclusions are specified using `exclude*` attributes, and the rule triggering condition assumes that the conditions hidden from the user are satisfied and that none of the specified exclusions are a match.

For example:

```
detection:
   exclude1:
     Image|endswith:
       - '\chrome.exe'
       - '\tor.exe'
   exclude2:
```

```
    QueryName|endswith: 'api.parsec.app'
  condition: not 1 of exclude*
```

Object isolation and backup

This section provides information about backing up detected malicious objects before they are disinfected or removed, and information about quarantining probably infected objects.

Isolating probably infected objects. Quarantine

When responding to threats, Kaspersky Industrial CyberSecurity for Nodes may create *Move file to Quarantine* tasks. This is necessary to minimize the consequences of the threat. Quarantine is a special local storage on the computer. The administrator can quarantine files that he/she considers dangerous for the computer. Quarantined files are stored in an encrypted state and do not threaten the security of the device. Kaspersky Industrial CyberSecurity for Nodes uses the quarantine only when working together with Kaspersky Industrial CyberSecurity Endpoint Detection and Response, Endpoint Detection and Response Expert (on-premises), or Kaspersky Industrial CyberSecurity for Networks. In other cases Kaspersky Industrial CyberSecurity for Nodes places the relevant file in Backup.

You can create *Move file to Quarantine* tasks in the following ways:

- In the alert details (only for Kaspersky Industrial CyberSecurity Endpoint Detection and Response).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For more information about managing alert details, refer to the Kaspersky Industrial CyberSecurity Endpoint Detection and Response Help.

- Using the Task Wizard.

  You must enter a file path or a checksum and a folder path.

The Move file to Quarantine task has the following limitations:

- The file size must not exceed 100 MB.
- System Critical Objects (SCO) cannot be quarantined. SCOs are files that the operating system and the Kaspersky Industrial CyberSecurity for Nodes application require to be able to run.
- You can manage task settings for Kaspersky Industrial CyberSecurity Endpoint Detection and Response in the Web Console.

How to create a Move file to Quarantine task in the Web Console

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

   The list of tasks opens.

2. Click **Add**.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Industrial CyberSecurity for Nodes**.

   b. In the **Task type** drop-down list, select **Move file to Quarantine**.

   c. In the **Task name** field, enter a brief description of the task and click **Next**.

4. In the **Task scope** section, select managed devices and click **Next**.
5. Enter the account credentials of the user whose rights you want to use to run the task. Click **Next**.
   By default, Kaspersky Industrial CyberSecurity for Nodes starts the task as the system user account (SYSTEM).
6. Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.
7. Click the new task. The task properties window opens.
8. Select the **Application settings** tab.
9. In the list of files, click **Add**. The file adding wizard starts.
10. To add the file, you must enter the full path to the file, or checksum with a folder path.

    If the file is located on a network drive, enter the file path starting with \\, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, you can get a File not found error.

11. In the task properties window, select the **Schedule** tab. Configure the task schedule.

    Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

12. Click **Save**.
13. Select the check box next to the task and click the **Start** button.

As a result, Kaspersky Industrial CyberSecurity for Nodes moves the file to Quarantine.

If the file is locked by a different process, the task is displayed as **Passed**, but the file itself is quarantined only after the computer is restarted. After restarting the computer, confirm that the file is deleted.

The *Move file to Quarantine* task can finish with the *Not enough space in Quarantine storage* error if you are trying to quarantine a file that is too large. Empty the Quarantine or increase its size. Then try again.

You can restore a file from Quarantine or empty the Quarantine using Web Console.

Viewing quarantine objects

You can view quarantined objects in the Kaspersky Security Center Administration Console and Web Console.

How to view quarantined objects in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.
3. Go to the **Quarantine** folder.
4. Information about quarantined objects is displayed in the right pane of the console.

How to view quarantined objects in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Quarantine** folder.
4. Information about quarantined objects is displayed in the right pane of the console.

To find the required object in the list of quarantined objects,

Sort or filter the objects.

Sorting quarantined objects

By default, objects in the list of quarantined objects are sorted by quarantine date in reverse chronological order. To find the required object you may sort objects by the columns with object information. To sort objects:

How to sort files in Quarantine in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Quarantine**.
3. In the list of files select the column heading which you want to use to sort the objects.

Files in Quarantine will be sorted based on the selected criterion.

How to sort files in Quarantine in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Quarantine**.
3. In the list of files select the column heading which you want to use to sort the objects.

Files in Quarantine will be sorted based on the selected criterion.

Filtering quarantined objects

To find the required quarantined object, you can filter objects in the list, i.e. display only those objects that satisfy the filtering criteria (filters) that you specify.

How to filter files in Quarantine in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.

3. Go to the **Quarantine** folder.
4. In the right pane, click the **No filter specified,** link.
5. Click **Adjust filter** and in the **Filtering settings** window, select columns for filtering.
6. Specify operators and values for the selected columns.
7. The created filters will be saved.
8. To display all quarantine objects again, in the **Filtering settings** window, click **Clear all**.

How to sort files in Quarantine in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Quarantine** folder.
4. Click the filter icon and click the **Add** button on the **Filters** tab.
5. Select a property to filter by.
6. Specify a condition and a value for the selected property.
7. Click **Apply**.
   Filter settings are saved.
8. To restore the display of all quarantined objects, click **Clear all** on the **Filters** tab.

Restoring quarantined objects

Kaspersky Industrial CyberSecurity for Nodes places probably infected objects into the Quarantine folder in encrypted form to shield the protected device against any possible harmful effects.

You can restore any object from Quarantine if you consider the object safe for the protected device and want to use it. If you do not want Kaspersky Industrial CyberSecurity for Nodes to isolate the object during the subsequent scans, you can exclude the object from processing in the Real-Time File Protection component and On-Demand Scan tasks, or you can add the object to the trusted zone.

Restoring objects from Quarantine may lead to an infection of the protected device.

You can restore one or more objects.

Restoring objects from Quarantine in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select the **Additional** → **Storages** folder.
2. Go to the **Quarantine** folder.

3. Do one of the following:

    - To restore one object, select **Restore** in the context menu of the name of the object.
    - To restore multiple objects, select the objects that you want to restore using the CTRL or SHIFT key, right-click one of the selected objects, and select **Restore** from the context menu.

4. The object will be restored to the original folder.

Restoring objects from Quarantine in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Quarantine** folder.
4. Select objects from the list and click the **Restore** button.
5. The object will be restored to the original folder.

Deleting objects from Quarantine

You can delete objects from Quarantine in the Kaspersky Security Center Administration Console and Web Console.

How to delete objects from Quarantine in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.
3. Go to the **Quarantine** folder.
4. Do one of the following:

    - To delete one object, select **Delete** in the context menu of the object.
    - To delete multiple objects, select the objects that you want to delete using the CTRL or SHIFT key, right-click one of the selected objects, and select **Delete** from the context menu.

5. The objects will be deleted from Quarantine.

How to delete objects from Quarantine in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Quarantine** folder.
4. Select objects from the list and click the **Delete** button.

5. Confirm the deletion.

6. The selected objects are deleted from Backup.

Sending probably infected objects to Kaspersky for analysis

If the behavior of an object gives you a reason to suspect that it contains a threat, and Kaspersky Industrial CyberSecurity for Nodes considers the object to be clean, you may have encountered an unknown threat whose signature has not yet been added to the databases. You can send this object to Kaspersky for analysis. Kaspersky's Anti-Virus analysts will analyze it and, if they detect a new threat, will add a record identifying it in the databases. When you rescan the object after the database has been updated, it is likely that Kaspersky Industrial CyberSecurity for Nodes will identify the object as infected and will be able to disinfect it. You will not only be able to keep the object, but will also prevent a virus outbreak.

To send an object for analysis to Kaspersky experts in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.

2. In the console tree, select **Additional** → **Storages**.

3. Go to **Quarantine** or **Backup** folder.

4. Do one of the following:

   - To send one object, select **Send to Kaspersky** in the context menu of the name of the object.

   - To send multiple objects, select the objects that you want to send using the CTRL or SHIFT key, right-click one of the selected objects, and select **Send to Kaspersky** from the context menu.

5. Select the folder for saving the object on your computer.

6. After this, you are prompted to go to the Kaspersky Threat Intelligence Portal and upload the saved object to get full information about it.

To send an object for analysis to Kaspersky experts in the Kaspersky Security Center Web Console

1. Open the Web Console.

2. In the console tree, select **Operations** → **Storages**.

3. Go to **Quarantine** or **File backups** folder.

4. Select objects from the list and click the **Send to Kaspersky** button.

5. Select the folder for saving the object on your computer.

6. After this, you are prompted to go to the Kaspersky Threat Intelligence Portal and upload the saved object to get full information about it.

Kaspersky Security Center Web Console or Administration Console cannot be used to send Quarantine and Backup objects to Kaspersky for analysis if they were migrated after upgrading version 4.0 or earlier of the application to 4.5 or later, or if the objects were placed in storages by Kaspersky Anti Targeted Attack Platform or Kaspersky Industrial CyberSecurity for Networks scenarios.

Configuring Quarantine settings

You can configure Quarantine settings. New Quarantine settings are applied immediately after saving.

How to configure Quarantine settings in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Supplementary** → **Storages** and click **Settings**.
4. Select the **Quarantine** tab.
5. Specify the Quarantine settings (see the table below).
6. Save your changes.

How to configure Quarantine settings in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Supplementary** → **Storages** and click the **Configure** button.
5. Go to the **Quarantine** tab.
6. Specify the Quarantine settings (see the table below).
7. Save your changes.

Quarantine settings

Parameter	Description
Limit the size of Quarantine to	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes monitors the total size of objects placed in Quarantine. If the specified value is exceeded (the default value is 1024 MB), Kaspersky Industrial CyberSecurity for Nodes logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type. Meanwhile the application stops quarantining new objects. You must empty the Quarantine manually. If this functionality is disabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the total size of objects placed in Quarantine. By default, the functionality is disabled.
Threshold value for available space	If the check box is selected, Kaspersky Industrial CyberSecurity for Nodes monitors the minimum amount of free space in Backup (the default value is 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Quarantine free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. The **Threshold value for available space** check box is active if the **Limit the size of Quarantine to** check box is selected. This option is enabled by default.

Making backup copies of objects. Backup

Kaspersky Industrial CyberSecurity for Nodes saves encrypted copies of disinfected or deleted objects in the Backup folder.

If the object is a part of a compound object (for example, part of an archive), Kaspersky Industrial CyberSecurity for Nodes will save the compound object in its entirety in Backup. For example, if Kaspersky Industrial CyberSecurity for Nodes has detected that one of the objects from a mail database is infected, it will back up the entire mail database.

Large objects placed in Backup by Kaspersky Industrial CyberSecurity for Nodes can slow down the system and reduce available disk space on the hard drive.

Files can be restored from Backup either to their original folder or to a different folder on the protected device. A file can be restored from Backup, for example, if an infected file contains important information, but Kaspersky Industrial CyberSecurity for Nodes is unable to disinfect it without damaging its integrity and losing the information.

Restoring files from Backup may lead to an infection of the protected device.

Viewing objects in Backup

This section provides information on how to view the list of files in Backup.

How to view Backup objects in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.
3. Go to the **Backup** folder.
4. Information about objects placed in Backup is displayed in the right pane of the console.

How to view Backup objects in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Backup** folder.
4. Information about objects placed in Backup is displayed in the right pane of the console.

How to view Backup objects in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. Information about objects placed in Backup is displayed in the right pane of the console.

To find the necessary object in the list of objects in Backup,

Sort or filter the objects.

Sorting files in Backup

By default, files in Backup are sorted by the backup date in reverse chronological order. To find the required file, you can sort files according to the content of any column in the results pane.

How to sort files in Backup in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.
3. Go to the **Backup** folder.
4. In the list of files select the column heading which you want to use to sort the objects.

Files in Backup will be sorted based on the selected criterion.

How to sort files in Backup in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Backup** folder.
4. In the list of files select the column heading which you want to use to sort the objects.

Files in Backup will be sorted based on the selected criterion.

How to sort files in Backup in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. In the list of files select the column heading which you want to use to sort the objects.

Files in Backup will be sorted based on the selected criterion.

Filtering files in Backup

To find a file in Backup, you can filter files to have the list display only those files which satisfy the filtering criteria (filters) that you have specified.

Filtering files in Backup in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Supplementary** → **Storages**.
3. Go to the **Backup** folder.
4. In the right pane, click the **No filter specified,** link.
5. Click **Adjust filter** and in the **Filtering settings** window, select columns for filtering.
6. Specify operators and values for the selected columns.
7. The created filters will be saved.
8. To display all objects in Backup again, in the **Filtering settings** window, click **Clear all**.

Filtering files in Backup in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Backup** folder.
4. Click the filter icon and click the **Add** button on the **Filters** tab.
5. Select a property to filter by.
6. Specify a condition and a value for the selected property.
7. Click **Apply**.
   Filter settings are saved.
8. To display all objects in Backup again, on the **Filters** tab, click **Clear all**.

How to filter files in Backup in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. In the file table, select the heading of the column and click the filter icon in the upper left corner.
3. Configure the filter and click **OK**.
   Filter settings are saved.

Restoring files from Backup

Kaspersky Industrial CyberSecurity for Nodes stores files in the Backup folder in encrypted form to shield the protected device against possible harmful effects.

Any file can be restored from Backup.

A file may need to be restored in the following cases:

- The original infected file contained important information and Kaspersky Industrial CyberSecurity for Nodes failed to keep its integrity so, as a result, the information in the file became unavailable.
- You consider the file harmless to the protected device and want to use it. If you do not want Kaspersky Industrial CyberSecurity for Nodes to consider this file infected, during subsequent scans you can exclude it from processing in the Real-Time File Protection task and On-Demand Scan tasks.

Restoring files from Backup may lead to an infection of the protected device.

When you restore a file you can select where it will be saved: the original location (default), the special folder for restored objects on the protected device, or a custom folder on the protected device where the Application Console is installed.

By default when Kaspersky Industrial CyberSecurity for Nodes restores a file, it makes a copy of it in Backup. The file copy can be deleted from Backup after it is restored.

Restoring files from Backup in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select the **Additional** → **Storages** folder.
2. Go to the **Backup** folder.
3. Do one of the following:
   - To restore one object, select **Restore** in the context menu of the name of the object.
   - To restore multiple objects, select the objects that you want to delete using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Restore** from the context menu.
4. The object will be restored to the original folder.

Restoring files from Backup in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Backup** folder.
4. Select objects from the list and click the **Restore** button.
5. The object will be restored to the original folder.

Restoring files from Backup in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. Perform one of the following actions in the results pane of the **Backup** node:
   - To restore one object, select **Restore** from the context menu of the object that you want to restore.
   - To restore multiple objects, select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Restore** from the context menu.
3. In the **Restore object** window, specify the folder in which the object being restored will be saved for each selected object.

   The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed.

4. Do one of the following:
   - To restore an object to its original location, select **Restore to the source folder**.
   - To restore an object to the folder specified as the location for restored objects during application installation, select **Restore to the default folder for restoration**.
   - To save an object to a different folder on the protected device where the Application Console is installed, select **Restore to a folder on your local computer** and then select the required folder or specify the path to it.
5. If you do not want to save a copy of the file in the Backup folder after it is restored, select the **Remove objects from storage after they are restored** check box (by default, this check box is cleared).
6. To apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.
7. Click **OK**.
8. Kaspersky Industrial CyberSecurity for Nodes will start restoring the first of the selected objects.
9. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.
   a. Select one of the following Kaspersky Industrial CyberSecurity for Nodes actions:
      - **Replace**, to replace the existing object with the restored object.
      - **Rename**, to save the restored object under a different name. In the entry field, enter the new restored object's filename and full path.
      - **Rename by adding suffix**, to rename the restored object by adding a suffix to its filename. Enter the suffix in the entry field.
   b. If you selected several objects to be restored, then select the **Apply to all selected objects** check box to apply the selected action (**Replace** or **Rename**) to the rest of the selected objects. If you selected **Rename**, the **Apply to all selected objects** check box will be unavailable.

c. Click **OK**.

The object will be restored. Information about the restoration operation will be recorded in the system audit log.

If you did not select **Apply to all selected objects** in the **Restore object** window, the **Restore object** window may open again. Use this window to specify the location where the next selected object will be saved.

Deleting files from Backup

Deleting files in Backup in the Kaspersky Security Center Administration Console

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select **Additional** → **Storages**.
3. Go to the **Backup** folder. The right pane displays the list of objects in Backup.
4. Do one of the following:
   - To delete one object, select **Delete** in the context menu of the object.
   - To delete multiple objects, select the objects that you want to delete using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Delete** from the context menu.
5. The selected objects are deleted from Backup.

Deleting files from Backup in the Kaspersky Security Center Web Console

1. Open the Web Console.
2. In the console tree, select **Operations** → **Storages**.
3. Go to the **Backup** folder.
4. Select objects from the list and click the **Delete** button.
5. The selected objects are deleted from Backup.

Removing files from Backup in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. The right pane displays the list of objects in Backup.
3. Do one of the following:
   - To delete one object, select **Delete** in the context menu of the object.
   - To delete multiple objects, select the objects that you want to delete using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Delete** from the context menu.
4. The selected objects are deleted from Backup.

Configuring Backup settings

How to configure Backup settings in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Supplementary** → **Storages** and click **Settings**.
4. Go to the **Backup** tab.
5. Specify the Backup settings (see the table below).
6. Save your changes.

How to configure Backup settings in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Supplementary** → **Storages** and click the **Configure** button.
5. Go to the **Backup** tab.
6. Specify the Backup settings (see the table below).
7. Save your changes.

How to configure Backup settings in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. In the results pane of the **Backup** node, click **Properties**.
3. In the **Properties: Backup** window, specify the Backup settings (see the table below).
4. Save your changes.

Backup settings

Parameter	Description
Store objects no longer than	If this functionality is enabled, the maximum file storage term is limited to the defined time interval. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Industrial CyberSecurity for Nodes deletes the oldest files from Backup.
Limit the size of Backup to	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes monitors the total size of objects placed in Backup. If the specified value is exceeded (the default value is 400 MB), Kaspersky Industrial CyberSecurity for Nodes logs the *Maximum Backup size exceeded* event and issues a notification according to the settings for notifications about events of this type. If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes does not monitor the total size of objects placed in Backup. By default, the functionality is disabled.
Limit threshold value for available space to	If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes monitors the minimum amount of free space in Backup (the default value is 100 MB). If the amount of free space decreases below the specified threshold, Kaspersky Industrial CyberSecurity for Nodes logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type. The **Limit threshold value for available space to** check box is active if the **Limit the size of Backup to** check box is selected. This option is enabled by default.

If the size of objects in Backup exceeds the maximum Backup size or exceeds the available space threshold, Kaspersky Industrial CyberSecurity for Nodes will notify you about this while continuing to place objects in Backup.

Backup statistics

You can view information about the current status of Backup, i.e. Backup statistics.

To view Backup statistics:

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Storages** → **Backup**.
2. In the results pane of the **Backup** node, click **Statistics**.

   This opens the **Backup. Statistics** window. The **Backup: Statistics** window displays information about the current Backup status (see the table below).

Information about the current Backup status

Field	Description
Current backup size	Total size of data in the Backup folder; the application calculates the file size in encrypted form.
Total number of objects	Current total number of objects in Backup.

Eliminating unprocessed threats

Kaspersky Industrial CyberSecurity for Nodes records information about files that for any reason were not processed. This information is recorded in the form of events in the list of active threats.

An infected file is considered *processed* if Kaspersky Industrial CyberSecurity for Node disinfected the file or removed the threat as part of scanning the computer for viruses and other malware. If Kaspersky Industrial CyberSecurity for Nodes does not perform an action on this file according to the specified application settings, the file will be added to the list of active threats.

If Kaspersky Industrial CyberSecurity for Nodes has any unprocessed threats, the device status will be changed to *Critical* in the Kaspersky Security Center console.

You can process active threats in the Administration Console and Web Console.

To process active threats in the Kaspersky Security Center console, you must enable the transmission of data on unprocessed files to Administration Server. Data transfer is enabled by default.

How to process a threat in the Kaspersky Security Center Administration Console

1. In the Administration Console, go to the folder **Administration Server → Advanced → Repositories → Active threats**.

   The list of active threats opens.

2. Select the object that you want to process.

3. Choose how you want to handle the threat:

   - **Disinfect**. If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application deletes the file.

   - **Delete**. If this option is selected, the application deletes infected file that are detected from active threats repository. In this case, the application keeps the detected file in the computer's memory. To eliminate the threat from the computer, select **Disinfect**.

How to process a threat in the Web Console

1. In the main window of the Web Console, select **Operations → Repositories → Active threats**.

   The list of active threats opens.

2. Select the object that you want to process.

3. Choose how you want to handle the threat:

   - **Disinfect**. If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application deletes the file.

   - **Delete**. If this option is selected, the application deletes infected file that are detected from active threats repository. In this case, the application keeps the detected file in the computer's memory. To eliminate the threat from the computer, select **Disinfect**.

Blocking access to network resources. Blocked network sessions

This section describes how to block remote devices and configure the settings for the List of blocked network sessions.

List of blocked network sessions

By default, the List of blocked network sessions is available for use if any of the following components is installed: Network Threat Protection or Anti-Cryptor. These components discover remote attempts to encrypt, open or execute objects on the protected device or network attached storage shared folders in accordance with the list of blocked network sessions. Information about blocked network sessions from all protected devices is sent to the Kaspersky Security Center. Kaspersky Industrial CyberSecurity for Nodes blocks current session and, in terms of current session, makes shared folders or network attached storage folders unavailable.

The List of blocked network sessions is populated when at least one of the following tasks is started in active mode (under specified conditions):

- For the *Network Threat Protection* task: activity typical of network attacks is detected.

  Kaspersky Industrial CyberSecurity for Nodes clears the block list when the application is restarted and when the Network Threat Protection settings are changed.

- For the *Anti-Cryptor* task: malicious encryption by a device accessing network file resources is detected.

After malicious activity or an encryption attempt is detected, the task sends information about the attacking network session to the List of blocked network sessions and the application creates a *Warning* event for current session of the attacking host. Any attempts by this session to access the protected shared network folders will be blocked.

If the locally unique identifier (LUID) of a host that initiated the attacking network session is added to the List of blocked network sessions, Kaspersky Industrial CyberSecurity for Nodes determines the IP address of the host and adds it to the List of blocked network sessions instead of the LUID of the attacking host.

By default, Kaspersky Industrial CyberSecurity for Nodes removes blocked network sessions from the list 30 minutes after they were added to the list. Access to network file resources is restored automatically after the network sessions are deleted from the List of blocked network sessions. You can specify the period of time after which blocked network sessions are automatically unblocked.

Note that when you restrict access to storage management for any user account, the List of blocked network sessions will still be available. The settings for blocked network sessions cannot be changed unless the selected user account has **Edit permissions** for managing Kaspersky Industrial CyberSecurity for Nodes.

Managing the list of blocked network sessions

To add network sessions showing any malicious or encrypting activity to the List of blocked network sessions and block access to network file resources for those sessions, at least one of the following components should be enabled:

- Network Threat Protection
- Anti-Cryptor

Enabling blocking of untrusted hosts in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Network activity control** → **Network Threat Protection settings** and click **Settings**.
4. In the window that opens, select the **Network Threat Protection** check box.
5. On the **General** tab, enable the **Block** mode.
6. Select the **Block attacking devices for** check box and specify the blocking duration.
7. Save your changes.

To configure the blocking of untrusted network sessions for the Anti-Cryptor component in policy properties:

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy window, select **Real-Time Computer Protection** → **Anti-Cryptor** and click **Settings**.
4. In the window that opens, select the **Anti-Cryptor** check box.
5. Go to the **Protection of shared folders** tab and select the **Protect shared folders** check box.
6. Select **Block connection for** and specify the blocking duration.
7. If necessary, specify the protection scopes and exclusions by IP address and mask.
8. Save your changes.

Enabling blocking of untrusted hosts in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Network activity control** → **Network Threat Protection** and click the **Configure** button.
5. In the window that opens, select the **Enable Network Threat Protection** check box.
6. Enable the **Block** mode.
7. Select the **Block attacking devices for** check box and specify the blocking duration.
8. If necessary, specify exclusions by IP address.
9. Save your changes.

To configure the blocking of untrusted network sessions for the Anti-Cryptor component:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Real-Time Computer Protection** → **Anti-Cryptor** and click the **Configure** button.
5. In the window that opens, select the **Enable Anti-Cryptor** check box.
6. Go to the **Protection of shared folders** tab and select the **Enable protection of shared folders against external encryption** check box.
7. Select **Block connection** and specify the blocking duration in the **Upon detection of external encryption of shared folders.** section.
8. If necessary, specify the protection scopes and exclusions by IP address and mask.
9. Save your changes.

Enabling blocking of untrusted hosts in the Application Console

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection** → **Network Threat Protection**.
2. In the results pane of the **Network Threat Protection** node, click **Properties**.

   The **Properties: Network Threat Protection** window opens.
3. In the window that opens, select the **Network Threat Protection** check box.
4. On the **General** tab, enable the **Block** mode.
5. Select the **Block attacking devices for** check box and specify the blocking duration.
6. Save your changes.

To configure the blocking of untrusted network sessions for the Anti-Cryptor component:

1. In the Kaspersky Industrial CyberSecurity for Nodes Console tree, select **Real-Time Computer Protection** → **Anti-Cryptor**.
2. Click **Properties** in the results pane of the **Anti-Cryptor** node.
3. In the window that opens, select the **Anti-Cryptor** check box.
4. Go to the **Protection of shared folders** tab and select the **Protect shared folders** check box.
5. Select **Block connection for** and specify the blocking duration.
6. If necessary, specify the protection scopes and exclusions by IP address and mask.
7. Save your changes.

Configuring the list of blocked sessions in the Application Console

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Blocked network sessions** child node.
3. In the results pane, click the **Properties** button.
4. In the window that opens, select the **Block attacking devices for** check box and specify the blocking duration.
5. To restore access to all blocked network sessions, click **Unblock all** in the upper part of the window.

   All network sessions will be removed from the list and unblocked.
6. To remove network sessions from the list of blocked network sessions, in the list in the results pane, select one or more sessions and click **Unblock selected** in the upper part of the window.

   The selected network sessions are unblocked.

Event registration. Kaspersky Industrial CyberSecurity for Nodes logs

This section provides information about working with Kaspersky Industrial CyberSecurity for Nodes logs.

Ways to register Kaspersky Industrial CyberSecurity for Nodes events

Events of Kaspersky Industrial CyberSecurity for Nodes are divided into two groups:

- Events related to the operation of application components, processing of objects in Kaspersky Industrial CyberSecurity for Nodes tasks.
- Events related to the administration of Kaspersky Industrial CyberSecurity for Nodes, such as starting the application, creating or deleting tasks, or editing task settings.

Kaspersky Industrial CyberSecurity for Nodes uses the following methods to log events:

- **Application components operation logs**. Logs contain information about events that occurred during the operation of application components.
- **System audit log**. The system audit log contains information about events related to the administration of Kaspersky Industrial CyberSecurity for Nodes. And also contains information about events associated with security breaches or attempted security breaches on the protected device.
- **Event Log**. The Event Log contains information about events required to diagnose failures in the operation of Kaspersky Industrial CyberSecurity for Nodes. The Event Log is available in Microsoft Windows Event Viewer.

Files that can be downloaded by the following links contain tables with the full lists of Kaspersky Industrial CyberSecurity for Nodes events of the following categories:

- Events that Kaspersky Industrial CyberSecurity for Nodes writes to the Event Log.

  DOWNLOAD WEL-EVENTS.ZIP
- Events that Kaspersky Industrial CyberSecurity for Nodes sends to the Administration Server.

  DOWNLOAD KSC-EVENTS.ZIP

Configuring the log settings

You can edit the following settings of Kaspersky Industrial CyberSecurity for Nodes logs:

- Length of the storage period for events in task logs and the system audit log.
- Location of the folder in which Kaspersky Industrial CyberSecurity for Nodes stores task log files and the system audit log file.
- Events generation thresholds for *Databases are out of date*, *Databases are extremely out of date* and *Critical areas scan has not been performed for a long time*.
- Events that Kaspersky Industrial CyberSecurity for Nodes saves in task logs, the system audit log, and the event log of Kaspersky Industrial CyberSecurity for Nodes in Event Viewer.
- Events that Kaspersky Industrial CyberSecurity for Nodes sends to the SIEM server.

How to configure the log settings in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Logs and notifications**.
4. In the **Task logs** section, click **Settings**.
   The **Notifications** window opens.
5. In this window, select the log that you want to configure and specify settings for individual events:
   - Where the events are saved: local report or Windows Event Log.
   - Event notifications: Notify by email, Notify by using terminal service, and/or Notify by running executable file.
   - Whether you want to send the event to a SIEM server and/or to Kaspersky Security Center.
6. Configure event generation thresholds by clicking **Event generation thresholds settings**.
7. This opens a window; in that window, specify the number of days after which the following events must be registered: *Databases are out of date*, *Databases are extremely out of date*, and *Critical areas scan has not been performed for a long time*.
8. Configure email notifications by clicking **Email notification settings**.
9. Save your changes.

How to configure the log settings in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.
   The policy properties window opens.

3. Select the **Application settings** tab.
4. Go to **Logs and notifications** → **Task logs** and click the **Configure** button.
5. This opens a window; in this window, on the **Notifications** tab, select the log that you want to configure and specify settings for individual events:
   - Where the events are saved: local report or Windows Event Log.
   - Event notifications: Notify by email, Notify by using terminal service, and/or Notify by running executable file.
   - Whether you want to send the event to a SIEM server and/or to Kaspersky Security Center.
6. Configure email notifications on the **Email notification settings** tab.
7. Save your changes.

How to configure the log settings in the Application Console:

1. In the Application Console tree, open the context menu of the **Logs and notifications** node.
2. Select **Properties**.
   The **Notifications** window opens.
3. In this window, select the log that you want to configure and specify settings for individual events:
   - Where the events are saved: local report or Windows Event Log.
   - Event notifications: Notify by email, Notify by using terminal service, and/or Notify by running executable file.
   - Whether you want to send the event to a SIEM server and/or to Kaspersky Security Center.
4. Configure event generation thresholds by clicking **Event generation thresholds settings**.
5. This opens a window; in that window, specify the number of days after which the following events must be registered: *Databases are out of date (days)*, *Databases are extremely out of date (days)*, and *Critical areas scan has not been performed for a long time (days)*.
6. Configure email notifications by clicking **Email notification settings**.
7. Save your changes.

Sorting events in the log

By default, events in the log are displayed in reverse chronological order.

To sort events in the log:

1. In the Application Console tree, open the context menu of the **Logs and notifications** node.
2. Select the required log.
3. In the results pane, select the header of the column that you want to use to sort the events in the list.

The sorted results will be saved for the next time you view the log.

Filtering events in the log

You can configure the log to display only the records of events that meet the filtering conditions (filters) that you have specified.

To filter events in the log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the log for which you want to configure a filter, and in the results pane, click **Filter**.

   The **Filter settings** window opens.
3. To add a filter, perform the following steps:

   a. In the **Field name** list, select the column you want to use to filter events.

   b. In the **Operator** list, select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.

   c. In the **Field value**, select a value for the filter.

   d. Click **Add**.

   The filter you added will appear in the list of filters in the **Filter settings** window.
4. If necessary, perform one of the following actions:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **OK** button to save the filtering conditions for log events.

The list of events of the log displays only events that meet the filtering conditions. The filtered results will be saved for the next time you view the log.

To disable the filter:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the log for which you want to remove a filter, and click **Remove filter**.

The log will then display all events.

Deleting events from the log

By default, Kaspersky Industrial CyberSecurity for Nodes retains log records for 30 days. You can change the storage period for records in a log.

To delete events from the log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the log from which you want to delete events, and in the results pane, click **Clear**.
3. Confirm the clearing operation.

The log is cleared.

Exporting information from the log

You can export data from logs into a CSV or TXT file.

To export events from logs:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select a log and in the results pane, click the **Export log** button.
   The **Save as** window opens.
3. Specify the name, location, and type of the file to which you want to export data from the log.
4. Click **Save**.

Information from the logs is saved to the specified file.

System audit log

Kaspersky Industrial CyberSecurity for Nodes performs a system audit of events related to the administration of Kaspersky Industrial CyberSecurity for Nodes. The application logs information about start of the application, starts and stops of Kaspersky Industrial CyberSecurity for Nodes tasks, changes in task settings, and creation and deletion of On-Demand Scan tasks. The application also logs information about events associated with security breaches or attempted security breaches on the protected device. Records of all those events are displayed in the results pane when you select the **System Audit** node in the Application Console.

By default, Kaspersky Industrial CyberSecurity for Nodes stores records in the system audit log for 30 days. You can change the storage period for records in a log.

You can specify a folder that Kaspersky Industrial CyberSecurity for Nodes will use to store files containing system audit log other than the default one.

Component and task logs

Information about the operation of Kaspersky Industrial CyberSecurity for Nodes components and tasks is displayed in the Application Console in the results pane when you select a node with the component or task name in the **Logs and notifications** section.

By default, Kaspersky Industrial CyberSecurity for Nodes keeps records in the logs of components and tasks for 30 days. For tasks - from the moment of their completion. You can change the storage period for records in task logs and component logs.

You can specify a folder that Kaspersky Industrial CyberSecurity for Nodes will use to store files containing task logs and component logs, other than the default one. You can also select events that Kaspersky Industrial CyberSecurity for Nodes will record in task logs and component logs.

In task logs, you can view detailed information about all events that have occurred in tasks since they started, as well as task execution statistics and task settings.

To view statistics and information about a Kaspersky Industrial CyberSecurity for Nodes task:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select a task and in the results pane, select the **Statistics** tab.

Viewing statistics and information about a Kaspersky Industrial CyberSecurity for Nodes task in task logs

In task logs, you can view detailed information about all events that have occurred in tasks since they started, as well as task execution statistics and task settings.

To view statistics and information about a Kaspersky Industrial CyberSecurity for Nodes task:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select a task and in the results pane, select the **Statistics** tab.

Viewing the event log of Kaspersky Industrial CyberSecurity for Nodes in Event Viewer

You can view the event log of Kaspersky Industrial CyberSecurity for Nodes using the Microsoft Windows Event Viewer snap-in for Microsoft Management Console. The log contains events registered by Kaspersky Industrial CyberSecurity for Nodes and required to diagnose failures in its operation.

Events that will be registered in the event log can be selected based on the following criteria:

- **by event types**.
- **by level of detail**. The level of detail corresponds to the importance level of the events registered in the log (informational, important, or critical events). The most detailed is the Informational level, which registers all events. The least detailed is the Critical level, which registers only critical events.

To view the Kaspersky Industrial CyberSecurity for Nodes event log:

1. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

   Microsoft Management Console opens.

2. Select **File** > **Add or remove snap-in**.

   The **Add or remove snap-ins** window opens.

3. In the list of available snap-ins, select the **Event Viewer snap-in** and click the **Add** button.

   The **Select computer** window opens.

4. In the **Select computer** window, specify the protected device on which Kaspersky Industrial CyberSecurity for Nodes is installed, and click **OK**.

5. In the **Add and remove snap-ins** window, click **OK**.

   In the Microsoft Management Console tree, the **Event Viewer** node appears.

6. Expand the **Event Viewer** node and select the **Applications and Services Logs** > **Kaspersky Industrial CyberSecurity for Nodes** child node.

The Kaspersky Industrial CyberSecurity for Nodes event log opens.

Administrator and user notification methods

You can configure the application to notify the administrator and users who access the device about the following events in the operation of Kaspersky Industrial CyberSecurity for Nodes and the anti-virus protection status on the device.

- The administrator can receive information about events of selected types.
- LAN users who access a device and terminal device users can receive information about events of the *Object detected* type in the Real-Time File Protection task.

Administrator or user notifications can be activated using several methods:

- Terminal service tools.

  You can apply this method for notifying terminal protected device users if the protected device is used as terminal.

- Running an executable file.

  This method runs an executable file stored on the protected device's local drive when an event occurs.

- Sending by email.

  This method uses email to transmit messages.

You can create the text of a message for individual event types. It can include an information field to describe an event. By default, the application uses a default message to notify users.

Configuring administrator and user notifications

Event notification settings give you a choice of methods for configuring and composing a message text.

How to configure event notifications in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Logs and notifications**.
4. In the **Task logs** section, click **Settings**.

   The **Notifications** window opens.
5. Select the event for which you want to select a notification method, and click **Notification settings**.

   The **Notification settings** window opens.
6. For an email notification, on the **Email** tab, you can add the text of the event notification message.

   To add fields with information about an event, click the **Variable** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

   To restore the default event message text, click the **By default** button.
7. For a notification by running an executable file, on the **Executable file** tab, select a file on the local drive of the protected device or enter the full path to it. This file will be run on the protected device when the event occurs. Enter the user name and password which will be used to execute the file.

   System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.
8. For a notification using the terminal service, on the **Terminal service** tab, you can add the text of the event notification message.

   To add fields with information about an event, click the **Variable** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

   To restore the default event message text, click the **By default** button.
9. Save your changes.

How to configure event notifications in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.

4. Go to **Logs and notifications** → **Task logs** and click the **Configure** button.

5. This opens a window; in that window, click the event for which you want to select a notification method.

   The **Notification settings** window opens.

6. For an email notification, in the **Notify users** section, select the **By sending email** check box and add the text of the event notification message.

   To add fields with information about an event, click the **Add variable** button and select the relevant items from the list. Fields with event information are described in the table in this section.

   To restore the default event message text, click the **Reset** button.

7. For a notification by running an executable file, in the **Notify administrators** section, select the **By running executable file** check box and enter the full path to a file on a local disk of the protected device. This file will be run on the protected device when the event occurs. Enter the user name and password which will be used to execute the file.

   System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

8. For a notification using the terminal service, in the **Notify administrators** section, select the **By using terminal service** check box and add the text of the event notification message.

   To add fields with information about an event, click the **Add variable** button and select the relevant items from the list. Fields with event information are described in the table in this section.

   To restore the default event message text, click the **Reset** button.

9. Save your changes.

How to configure event notifications in the Application Console

1. In the Application Console tree, open the context menu of the **Logs and notifications** node.

2. Select **Properties**.

   The **Notifications** window opens.

3. Select the event for which you want to select a notification method, and click **Notification settings**.

   The **Notification settings** window opens.

4. For an email notification, on the **Email** tab, you can add the text of the event notification message.

   To add fields with information about an event, click the **Variable** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

   To restore the default event message text, click the **By default** button.

5. For a notification by running an executable file, on the **Executable file** tab, select a file on the local drive of the protected device or enter the full path to it. This file will be run on the protected device when the event occurs. Enter the user name and password which will be used to execute the file.

   System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

6. For a notification using the terminal service, on the **Terminal service** tab, you can add the text of the event notification message.

   To add fields with information about an event, click the **Variable** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

To restore the default event message text, click the **By default** button.

7. Save your changes.

Fields with event information

Variable	Description
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Importance level.
%OBJECT%	Object name (in Real-Time Computer Protection and On-Demand Scan tasks). The Software Modules Update task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	The name of the object according to the Virus Encyclopedia classification. This name is included in the full name of a detected object that Kaspersky Industrial CyberSecurity for Nodes returns on detecting an object. You can view the full name of a detected object in the task log.
%VIRUS_TYPE%	The type of detected object according to the Kaspersky classification, such as "virus" or "trojan". It is included in the full name of a detected object, which is returned by Kaspersky Industrial CyberSecurity for Nodes when it finds an object infected or probably infected. You can view the full name of a detected object in the task log.
%USER_COMPUTER%	In the *Real-Time File Protection* task, the name of the protected device of the user who accessed the object on the device.
%USER_NAME%	In the *Real-Time File Protection* task, the name of the user who accessed the object on the device.
%FROM_COMPUTER%	Name of the protected device where the notification originated.
%EVENT_REASON%	Reason the event occurred (some events do not have this field).
%ERROR_CODE%	Error code (only for the "internal task error" event).
%TASK_NAME%	Task name (only for events related to task performance).
%PROTOCOL%	The protocol that is being used.
%MESSAGE%	Text of the message.
%DEVICE_INSTANCEPATH%	Path to the instance of the device.
%DEVICE_VID%	Device vendor
%DEVICE_PID%	Type of the controller.
%DEVICE_SERIALNUMBER%	Serial number of the device.

Configuring email notifications

How to configure email notifications in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, select **Logs and notifications**.
4. In the **Task logs** section, click **Settings**.
   The **Notifications** window opens.
5. Click **Email notification settings**.
6. In the window that opens, select the **Send event notifications** check box.

7. Under **Sending notifications on behalf of**, specify sender information: sender address, SMTP server, SMTP server port, user name and password.
8. Under **Notification recipient**, specify the recipient email address.
9. To test the settings, click the **Send test message** button.

   The test message functionality is available only in the Kaspersky Security Center Administration Console and the Application Console.

10. Specify the send mode: **If event occurs** or **By schedule (schedule not specified)**. To configure the schedule, click **Edit**.
11. Save your changes.

How to configure email notifications in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Logs and notifications** → **Task logs** and click the **Configure** button.
5. This opens a window; in that window, select the **Email notification settings** tab.
6. Select the **Send event notifications** check box.
7. Specify sender information: sender address, SMTP server, SMTP server port, user name and password.
8. Specify the recipient email address.
9. Specify the send mode: **If events occur** or **By schedule**. If applicable, configure the schedule.
10. Save your changes.

How to configure email notifications in the Application Console

1. In the Application Console tree, open the context menu of the **Logs and notifications** node.
2. Select **Properties**.

   The **Notifications** window opens.
3. Click **Email notification settings**.
4. In the window that opens, select the **Send event notifications** check box.
5. Under **Sending notifications on behalf of**, specify sender information: sender address, SMTP server, SMTP server port, user name and password.
6. Under **Notification recipient**, specify the recipient email address.

7. To test the settings, click the **Send test message** button.

   The test message functionality is available only in the Kaspersky Security Center Administration Console and the Application Console.

8. Specify the send mode: **If event occurs** or **By schedule (schedule not specified)**. To configure the schedule, click **Edit**.

9. Save your changes.

Configuring interaction with the Administration Server

You must select the types of objects about which Kaspersky Industrial CyberSecurity for Nodes sends information to the Kaspersky Security Center Administration Server.

How to configure the integration with the Administration Server in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the **Logs and notifications** section, click the **Settings** button in the **Interaction with Administration Server** subsection.

4. This opens a window; in that window, choose the types of objects about which Kaspersky Industrial CyberSecurity for Nodes will send information to the Kaspersky Security Center Administration Server:

   - **About Quarantine files**
   - **About files in Backup**
   - **About unprocessed files**
   - **About installed devices**
   - **About a threat development chain**
   - **About PLC projects**

5. Save your changes.

   Kaspersky Industrial CyberSecurity for Nodes will send information about the selected object types to the Administration Server.

How to configure the interaction with the Administration Server in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. In the **Logs and notifications** section, click the **Configure** button in the **Interaction with Administration Server** subsection.

5. This opens a window; in that window, choose the types of objects about which Kaspersky Industrial CyberSecurity for Nodes will send information to the Kaspersky Security Center Administration Server:

   - **Quarantine files**
   - **Backup files**
   - **About unprocessed files**
   - **Blocked network sessions**
   - **Installed devices**
   - **Threat development chain**
   - **Versions of PLC projects**

6. Save your changes.

Configuring incident generation

The Administration Server database stores information about application events that occur on the managed protected devices.

How to configure incident generation in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, select **Logs and notifications**.

4. In the **Incidents** section, click **Settings**.

5. This opens a window; in that window, if necessary, edit the selection of events in the table below, which Kaspersky Industrial CyberSecurity for Nodes will use to generate incidents:

6. Save your changes.

   The incident generation settings are saved.

How to configure incident generation in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Logs and notifications** → **Incidents** and click the **Configure** button.

5. This opens a window; in that window, if necessary, edit the selection of events in the table below, which Kaspersky Industrial CyberSecurity for Nodes will use to generate incidents:

6. Save your changes.

   The incident generation settings are saved.

List of events for incident generation

Event	Default value
PLC project does not match reference project	Selected
Error matching PLC project to reference project	Selected
Error getting PLC project information	Selected
License expired	Not selected
End User License Agreement has been violated	Selected
Failed to update	Not selected
Databases are corrupted	Not selected
Databases are extremely out of date	Not selected
Databases are out of date	Not selected
Network session listed as untrusted	Selected
Application launch denied	Not selected
Statistics only mode: application launch denied	Selected
Error processing application launch	Not selected
Untrusted external device detected and restricted	Selected
Statistics only: untrusted external device detected	Selected
Error processing device connection	Selected
Infected or other object detected	Selected
Object detected (KSN-untrusted object found)	Selected
Object not disinfected	Not selected
Object not backed up	Not selected
Network attack detected	Not selected

Portable Auditor

Portable Auditor is an application that allows scanning devices for malware, scanning for vulnerabilities and performing a security settings audit, as well as recording incoming and outgoing traffic. Portable Auditor runs from a removable drive connected to the device and does not require installation on the device being scanned. This lets you use Portable Auditor to scan devices on which, for some reason, you are not able to install the Kaspersky Industrial CyberSecurity for Nodes application:

- Isolated devices
- Devices on which installation of Kaspersky Industrial CyberSecurity for Nodes is impossible for the following reasons:
  - Security policies of your organization
  - Restrictions imposed by device vendors
  - Technical limitations of devices and other factors
- Guest devices

Portable Auditor does not leave traces of its work on the scanned device: by default, all files created by the application during operation are stored on the removable drive. If necessary, you can write Portable Auditor to a protected removable drive. In this case, the application files are located on a read-only partition, which allows protecting them if the Portable Auditor removable drive is connected to an infected device. The scan results are saved on a protected section of the removable drive, which allows protecting them from unauthorized access.

Portable Auditor scans devices using the following tasks:

- *Malware Scan*. By default, Portable Auditor scans local hard drives, RAM, and startup objects for viruses and other threatening programs. If necessary, you can configure the scan scope yourself. When an infected object is detected, the application performs the action specified in the task settings.
- *Security Audit*. Portable Auditor scans devices for vulnerabilities, assesses the compliance of devices with operating system security requirements, and collects **information about device configuration.**

  Portable Auditor gathers the following information about the device:
  - Running services
  - Installed drivers
  - Scheduled tasks
  - Installed applications and patches
  - Names of shared network resources
  - Startup items
  - Device information (IP address, DNS name)

    - Local users and groups
    - Hardware
- *Network traffic recording*: Portable Auditor records inbound and outbound traffic from the device being scanned during the specified period and writes it to a file of the PcapNG format.

You can use the same instance of Portable Auditor to scan multiple devices in a row. Subsequently, you can use the Portable Auditor Console to manage the scan results of each device separately.

Based on the results of each task, the application generates a separate report that can be exported. You can also view the detected threats report in the Portable Auditor Console.

You can manage the Portable Auditor using the Portable Auditor Console or the command line.

Hardware and software requirements

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Creating Portable Auditor

To create a Portable Auditor, you will need:

- A device with the Kaspersky Industrial CyberSecurity for Nodes application with a valid license.
- License for Kaspersky Industrial CyberSecurity for Nodes Portable Auditor.
- A USB removable drive at least 2 GB in size or a supported secure removable drive:
    - Rutoken EDS 2.0 Flash
    - Rutoken EDS 3.0 Flash

Hardware requirements for the scanned device

You can scan devices that meet the following minimum requirements:

- Processor: 1 GHz single-core processor, Celeron III or higher, or VIA C3
- RAM: 256 MB
- Free hard drive space: 2GB

Software requirements for the protected device

You can scan devices running one of the following 32-bit or 64-bit Microsoft Windows operating systems:

- Windows 2000 Professional SP4 32-bit.
- Windows XP Professional SP2 32-bit / 64-bit
- Windows XP Professional SP3 32-bit
- Windows Vista SP2 32-bit / 64-bit
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32-bit / 64-bit
- Windows 8 Pro / Enterprise 32-bit / 64-bit
- Windows 8.1 Pro / Enterprise 32-bit / 64-bit
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit

- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-bit

Server operating systems:

- Windows Server 2003 SP1 Standard / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-bit
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2008 SP2 Standard / Enterprise 64-bit
- Windows Small Business Server 2011 Essentials / Standard 64-bit
- Windows MultiPoint Server 2011 64-bit
- Windows Server 2012 Foundation / Essentials / Standard 64-bit
- Windows Server 2012 R2 Foundation / Essentials / Standard 64-bit
- Windows Server 2016 Essentials / Standard 64-bit
- Windows Server 2019 RS5 Essentials / Standard 64-bit
- Windows Server 2022 21H2 64-bit
- Windows Server 2022 version 20348.350 64-bit
- Windows Server 2025 version 26100.1742 64-bit

Embedded systems:

- Windows XP Embedded Service Pack 3 32-bit
- Windows Embedded POSReady 7 32-bit / 64-bit
- Windows Embedded Standard 7 Service Pack 1 32-bit / 64-bit
- Windows Embedded 8 Standard 32-bit / 64-bit
- Windows Embedded 8.1 Industry Pro 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1507 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1607 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1803 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1809 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 1903 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 2004 32-bit / 64-bit

- Windows 10 IoT Enterprise Version 20H2 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 21H1 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 21H2 32-bit / 64-bit
- Windows 10 IoT Enterprise Version 22H2 32-bit / 64-bit
- Windows 11 IoT Enterprise Version 21H2 64-bit
- Windows 11 IoT Enterprise Version 22H2 64-bit
- Windows 11 IoT Enterprise Version 23H2 64-bit
- Windows 11 IoT Enterprise Version 24H2 64-bit
- Windows 11 IoT Enterprise Version 25H2 64-bit

Portable Auditor functionality limitations

Portable Auditor has the following limitations:

- On Windows 2000 Professional devices, only the *Malware Scan* task can be run. The *Security Audit* and *Network traffic recording* tasks cannot be run due to operating system limitations.
- On Windows XP Professional, Windows Vista, Windows Server 2003, and Windows XP Embedded devices, the *Network traffic recording* task cannot be run due to operating system limitations.
- Creating Portable Auditor on a secure removable drive and running Portable Auditor from a secure removable drive is not possible on Windows 2000 Professional, Windows XP Professional, Windows Vista, Windows Server 2003, Windows XP Embedded devices.

Creating Portable Auditor

To create Portable Auditor:

1. Connect a supported removable drive to the device with an installed Kaspersky Industrial CyberSecurity for Nodes with a valid license.

   To have the Rutoken removable drive displayed in the list of connected removable media on a computer running Windows Server 2022, you must replace the UMDF2 driver for USB card readers with the WUDF driver.

2. In the notification area, in the context menu of the application icon, select the **Compact Diagnostic Interface**.
3. In the Compact Diagnostic Interface window that opens, click the **Create Portable Auditor** link.

   The Portable Auditor Wizard starts. Follow the instructions of the Wizard.

To proceed to the next step of the wizard, click **Next >**.

Step 1. Importing settings

If necessary, import the Portable Auditor settings from a previously created XML file:

1. Click **Settings import**.
2. In the window that opens, select the XML file containing the Portable Auditor settings.
3. Click **Open**.

   The settings imported from the XML file will be displayed at the subsequent wizard steps. If necessary, you can change these.

Step 2. Adding a key file

To create Portable Auditor, you need a valid Kaspersky Industrial CyberSecurity for Nodes Portable Auditor license.

Add a key file:

1. Click **Select license file**.
2. In the window that opens, select the key file for Portable Auditor.
3. Click **Open**.

   The license information will be displayed in the current wizard window.

Step 3. Selecting Portable Auditor tasks

Select the tasks to be performed by Portable Auditor when started on the device:

- **Scan selected area with anti-virus databases**. If this functionality is enabled, Portable Auditor scans a selected area for viruses and other threats. Portable Auditor applies the default security level: **Inform**. This option is enabled by default.
- **Record traffic from all network interfaces**. If this functionality is enabled, Portable Auditor records inbound and outbound traffic from a device being scanned for a specified amount of time. This option is enabled by default.
- **Perform Security Audit**. If this functionality is enabled, Portable Auditor can, depending on the settings, scan a device for vulnerabilities, assess device security and operating system compliance, or collect device configuration data using rules written in OVAL and XCCDF. This option is enabled by default.

If necessary, you can configure the selection of tasks that the Portable Auditor will perform when running the scan.

Step 4. Configuring scan task settings

This step is available if at step 3, you selected the **Scan selected area with anti-virus databases** action.

1. By default, the following objects are added to the scan scope: **Local hard drives**, **System memory and processes**, and **Startup objects**.

   You can exclude an object from the scan scope without deleting it. To exclude an object, clear the check box to the left of its name. You can include the desired objects in the scan scope in the task settings.

   Objects excluded from the scan scope are not added to the list of exclusions and may be included in the scope of the *Malware Scan* task. For example, if you exclude a folder on a local hard drive but the **Local hard drives** object is included in the scan scope, that folder will be scanned by the task.

2. If necessary, you an add objects to the scan scope:

   a. Click **Add**.

   b. In the opened **Scan scope** window, select the type of object that you want to add:

   - **Predefined scope**, if you want the scan scope to include one of the predefined scopes on the protected device. Then in the drop-down list, select the desired scan scope.
   - **Disk, folder or network location**, to include a single drive or folder in the scan scope. Then select the required scope in the window, opened by the **Browse** button.

     When a local hard drive is added to the scan scope, Portable Auditor does not scan shared folders linked to it. If you want to include shared folders, you need to add them separately.

   - **File**, to include a single file in the scan scope. Then, in the **Browse** window that opens, select the file.

   c. Click **OK**.

   d. Repeat steps a–c for each scan object you add.

   Added objects are included in the scan scope by default. If necessary, exclude the item from the scan scope using the check box to the left of its name.

   e. If necessary, remove an object from the list by clicking the **Delete** button.

3. Configure the task settings:

   a. Click **Scan settings**.

   b. On the **General** tab, under **Scan objects**, select the objects that you want to include in the scan scope:

   - **All objects**. Portable Auditor scans all objects.
   - **Objects scanned by format**. Portable Auditor scans only infectable objects based on file format. Formats are added to the list by Kaspersky experts; the list is part of the databases of Kaspersky Industrial CyberSecurity for Nodes.
   - **Objects scanned by the list of extensions specified in anti-virus databases**. Portable Auditor scans only infectable objects based on file extension. Extensions are added to the list by Kaspersky experts; the list is part of the databases of Kaspersky Industrial CyberSecurity for Nodes.
   - **Objects scanned by specified list of extensions**. Portable Auditor scans only infectable objects based on file extension. You can create your own list of extensions by clicking **Edit**.
   - **Scan disk boot sectors**. If the check box is selected, Portable Auditor scans boot sectors and master boot records on hard drives and removable drives of the protected device. The check box is selected by default.
   - **Scan alternate NTFS streams**. Scanning of alternative file and folder streams on drives with the NTFS file system. If the check box is selected, Portable Auditor scans a potentially infected object and all NTFS streams associated with that object. If the check box is cleared, the application scans only the object that was detected and considered as probably infected. The check box is selected by default.

c. In the **Scan of compound objects** section, specify the types of compound objects that you want to include in the scan scope:

- **Archives**. Scanning of ZIP, CAB, RAR, and ARJ archives and other archive formats.
- **SFX archives**. Scanning of self-extracting archives.
- **Packed objects**. Scanning of executable files packed by binary code packers, such as UPX or ASPack.
- **Plain email**. Scanning of files in mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.
- **Email databases**. Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files. This option is available if the **Plain email** check box is selected.
- **Embedded OLE objects**. Scanning of objects embedded in files (such as Microsoft Word macros, or email message attachments).

d. Go to the **Additional** tab.

e. In the **General settings** block:

- **Restore file attributes after scanning**. If a file is opened during the scan, the last accessed time for the file is updated. As a result, the archivers and cloud storages recalculate file data to transfer it to a cloud or to a backup. To avoid the recalculation process, you can restore the last accessed time after scanning is performed. By default, the option is disabled.
- **Limit CPU usage for scan tasks**. This setting is used to avoid making the computer hang during scanning. This option may be crucial for industrial systems, where the main software is not supposed to freeze. By default, the option is disabled.
- **Folder for temporary files created during scanning**. By default, temporary files are saved in the kavscan\Results\<Name of the scanned device>\<date_time>\Temp folder, located on the removable drive with Portable Auditor. If necessary, you can change the folder for storing temporary files. For example, if the removable drive runs out of free space during scanning or the scan takes too long due to low read/write speeds, you can configure temporary files to be stored in a folder on the device being scanned.

f. Under **Action to perform on detected objects**, select the action that Portable Auditor will perform on infected and other detected objects:

- **Disinfect, delete if disinfection fails**. If this option is selected, the application automatically attempts to disinfect all infected files that are detected. If disinfection fails, the application deletes the files.
- **Inform** (default value). If this action is selected, Portable Auditor does not perform any actions on an infected object or other detected objects. The application only logs an event in the report. You can use this option for a quick scan or, for example, to scan systems in which industrial software modules must never be deleted.

g. If the **Disinfect, delete if disinfection fails** option is selected, configure the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** functionality. If this functionality is enabled, Portable Auditor forces the deletion of the entire parent compound object whenever a malicious or other nested object is detected. The parent file along with all of its contents are forcibly removed if the application cannot remove only the detected child object (for example, if the parent object cannot be modified). If this functionality is disabled, Portable Auditor does not delete the parent object. This option is enabled by default.

h. Go to the **Performance** tab.

i. Under **Exclusions**, if necessary, add exclusions from the scan scope:

- **Exclude files**. Use this functionality to exclude the files from scan scope and not remove them if detected. You can both specify a full path and use a mask. By default, the functionality is disabled.
- **Do not detect objects by type**. You can use this feature to prevent the detection and subsequent deletion of objects of a certain type. You can specify the object name or use a mask. By default, the functionality is disabled.

j. You can make the scan finish sooner and increase the speed of Portable Auditor using settings under **Advanced settings**:

- **Stop scanning if it takes longer than (sec)**. If this functionality is enabled and it takes too long to scan an object, Portable Auditor will stop scanning that object and continue scanning the area. You can use this option, for example, if Portable Auditor takes too long to scan large files or the network environment. This option is enabled by default. The default value is 60 seconds.
- **Do not scan compound objects larger than (MB)**. If this option is enabled, Portable Auditor excludes from scanning objects that are larger than the specified size. This option is enabled by default. The default value is 100 MB.
- **Use iChecker technology**. This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scans by using a special algorithm that takes into account the release date of Portable Auditor databases, the date when the file was last scanned, and any modifications to the scan settings. There are limitations to iChecker Technology: it does not work with large files and applies only to files with a structure that the application recognizes (for example, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, and RAR).

4. To create scan exclusions, click the **Exclusions settings** button.

The **Scan exclusions** window opens.

Portable Auditor does not scan folders and objects from the exclusion list, even if they are included in the scan scope. For example, if a hard drive is added to the list of exclusions, Portable Auditor will not scan the folders included in the scan scope located on that drive.

5. Create scan exclusions:

   a. Click **Add**.

   b. In the opened **Add scan exclusion** window, select the type of object that you want to add:

   - **Predefined scope**, if you want the list of exclusions to include one of the predefined scopes on the protected device. Then in the drop-down list, select the desired scan scope.
   - **Disk, folder or network location**, if you want the list of exclusions to include a single drive or folder in the scan scope. Then select the required scope in the window, opened by the **Browse** button.

     When a local hard drive is added to the list of exclusions, Portable Auditor does not exclude shared folders linked to it from the scan scope. If you want the list of exclusions to include shared folders, you need to add them separately.

   - **File**, to include a single file in the scan scope. Then, in the **Browse** window that opens, select the file.

   c. Click **OK**.

   d. Repeat steps a–c for all exclusions that you want to add.

   e. You can delete the added exclusion using the **Delete** button.

Step 5. Configuring network traffic recording

This step is available if at step 3, you selected the **Record traffic from all network interfaces** action.

If required, in the **Record inbound and outbound network traffic of the host being checked during the following time interval (sec)** field, change the period for Portable Auditor to record inbound and outbound traffic from the device being scanned. The default value is 30 seconds.

Step 6. Configuring security audit settings

This step is available if at step 3, you selected the **Perform Security Audit** action.

Select the OVAL and XCCDF rule sources that Portable Auditor will use to audit device security:

- **Kaspersky ICS CERT vulnerabilities database for SCADA**. Portable Auditor scans the device for all vulnerabilities described in the OVAL rules, in the Kaspersky ICS CERT for ICS vulnerability database. By default, the option is selected.
- **Rules for collecting host configuration data**. Portable Auditor gathers information about the device configuration. By default, the option is selected.

- **Compliance and security configurations for operating systems**. Portable Auditor checks the operating system settings of the device for compliance with security benchmarks. By default, the option is selected.

  It is not always known in advance which operating systems are installed on the scanned devices, so configurations for all supported operating systems are selected by default. If necessary, you can exclude unused configurations by clicking **Select configurations**.

  Kaspersky ICS CERT vulnerabilities database for SCADA, Rules for collecting host configuration data, and Compliance and security configurations for operating systems are provided with the Portable Auditor databases. Therefore, before starting Portable Auditor with at least one of the listed rule sources, make sure that the Portable Auditor databases are up to date.

- **Custom rule database**. Portable Auditor checks the device for vulnerabilities described in custom OVAL and XCCDF rules. If you select this option, you must upload a ZIP archive with a database of rules.

Step 7. Selecting a removable drive

Select the removable drive where Portable Auditor will be created:

- **Removable drive**. Removable USB drive. Select the removable drive from the drop-down list.
- **Secure removable drive**. Removable USB drive protected from reading, copying, and writing by the administrator password. If you have selected this option, select a secure removable drive at the next wizard step.

  You cannot use the same secure removable drive simultaneously for creating Portable Auditor and for securely copying application databases.

By default, Kaspersky Industrial CyberSecurity for Nodes verifies the Portable Auditor data. If you plan to create Portable Auditor with identical settings on multiple removable drives, verifying the data for the first Portable Auditor and detecting discrepancies early on can save you time. If necessary, disable this functionality by clearing the **Verify Portable Auditor data after creation** check box.

Step 8. Configuring the secure removable drive

This step is available if at step 7, you selected the **Secure removable drive** option.

Configure the settings for the secure removable drive:

1. Select the connected secure removable drive where Portable Auditor will be created.
2. Under **Security settings**, in the **Enter the current administrator PIN code** field, enter the administrator PIN code set on the secure removable drive to protect its contents.

   This PIN code will be requested in the future when performing any action with Portable Auditor.

3. If necessary, change the current administrator PIN:

   a. Select the **Change the current PIN code (only digits and Latin symbols are allowed)** check box.

   b. Enter a new PIN code in the appropriate field.

   c. Confirm the new PIN.

Step 9. Writing Portable Auditor to the removable drive

At this step, you can review all settings of Portable Auditor before proceeding with its creation. If necessary, you can export these settings to an XML file by clicking **Export**.

Click the **Finish** button to create Portable Auditor with the specified settings.

It is not recommended to connect two Rutoken removable drives to the same device and simultaneously running the Secure copying of application databases and Creating Portable Auditor tasks. In this case, the tasks may end with an error.

Portable Auditor will be written to the selected removable drive. A kavscan folder will appear on the removable drive, containing the files and folders required for Portable Auditor to work.

If Portable Auditor is already installed on the removable drive, the Wizard will overwrite all files of the existing Portable Auditor in the kavscan folder. If you decide to abort writing, the installation wizard terminates write operation without rolling back the changes made.

After you complete the setup, the wizard prompts you to create another Portable Auditor.

To avoid damaging data on the removable drive, use the safe removal feature when working with Portable Auditor.

You can also create Portable Auditor using the command line interface.

Updating Portable Auditor

To upgrade the Portable Auditor to a newer version, you need to connect the removable drive to a device on which the current version of Kaspersky Industrial CyberSecurity for Nodes is installed, and create the Portable Auditor from scratch.

When you upgrade the Portable Auditor, the scan results stored on the removable disk are deleted.

Working with the Portable Auditor Console

Portable Auditor Console cannot run if less than 200 KB of free space is left on the removable drive with Portable Auditor.

To start Portable Auditor Console on the device being scanned:

1. Connect the Portable Auditor removable drive to the device.
2. Go to the kavscan folder on the Portable Auditor removable drive.
3. Run the kavscan_ui.exe executable file.

   To run Portable Auditor tasks, a user must have administrator rights on the device being scanned.

4. If Portable Auditor is recorded on a secure removable drive, enter the PIN.

The Portable Auditor Console window is opened.

You can run only one instance of Portable Auditor Console on the device being scanned.

After launching the Portable Auditor Console, the **Dashboard** section is displayed. The following information about the application is displayed in this section:

- Under **Tasks**, you can view the current status of Portable Auditor tasks.
- Under **Statistics**, you can view statistics of this instance of Portable Auditor for the entire time since its creation:
  - **Last run** is the completion date of the last started task.
  - **Hosts scanned** is the number of unique devices on which at least one task has been run.
  - **Hosts with detected threats** is the number of scanned devices on which threats were detected.
  - **Malware Scan tasks** is the total number of running *Malware Scan* tasks.
  - **Security Audit tasks** is the total number of running *Security Audit* tasks.
  - **Network traffic recording tasks** is the total number of running *Network traffic recording* tasks.
- Under **Disk space**, you can view information about the available and used space on the removable drive.

To delete files created by Portable Auditor from the removable drive:

a. In the **Disk space** block, click the **Free up space** link.

In the window that is displayed, you can view detailed information about how much space (in MB) on the removable drive is occupied by Portable Auditor task reports, dump files, and trace files.

b. Click the **Delete** button in the appropriate section and confirm the action.

c. To delete all files, click the **Delete all** button and confirm the action.

Portable Auditor deletes the selected files from the removable drive.

You can also delete task report files for individual devices in the **Reports** section.

To exit the Portable Auditor Console:

From the context menu of the Portable Auditor icon in the system tray, select **Exit**.

When you close the Portable Auditor Console window, the application continues to run in the background.

To avoid damaging data on the removable drive, use the safe removal feature when working with Portable Auditor.

Device scan

Tasks cannot run if less than 100 MB of free space is left on the removable drive with Portable Auditor.

To run a device scan using Portable Auditor, follow these steps:

1. Start Portable Auditor Console on the device that you want to scan.

   To run Portable Auditor tasks, a user must have administrator rights on the device being scanned.

2. Go to the **Tasks** section.

   In the displayed window, you can view the current status of each task, the date and time of its last start, as well as the selected configuration method: **Default** or **Custom**.

   The default task settings are the settings specified when the Portable Auditor was created.

3. To start tasks with the current settings, select check boxes for the tasks that you want to start and click the **Run selected tasks** button. The default selection includes the tasks that were configured to run when the Portable Auditor was created.

   You can also start a single task by clicking the **Run** button in the appropriate section.

4. To specify custom settings for the task, click the **Settings** button in the appropriate section. To restore the default settings, click the **Restore default settings** link.

   If necessary, you can export and import task settings.

5. After starting the tasks, the application displays the current progress of the tasks. When running multiple tasks at the same time, Portable Auditor runs tasks sequentially one after another. You can stop task execution using the **Cancel** button.

After the tasks finish, Portable Auditor saves report files on the removable drive and displays information about the result in the **Status** field. You can proceed to viewing the scan results or exit Portable Auditor on the current device.

To avoid damaging data on the removable drive, use the safe removal feature when working with Portable Auditor.

You can also run a device scan using the command line.

Malware Scan task settings

To configure the Malware Scan task:

1. In the **Malware Scan** block, click the **Settings** button.

   The **Scan settings** window opens.

2. In the **Settings** field, select **Custom**.

3. On the **Scan scope** tab, configure the scan scope. By default, the scan scope includes objects that were included when Portable Auditor was created.

   You can exclude an object from the scan scope without deleting it. To exclude an object, clear the check box to the left of its name.

   Objects excluded from the scan scope are not added to the list of exclusions and may be included in the scope of the *Malware Scan* task. For example, if you exclude a folder on a local hard drive but the **Local hard drives** object is included in the scan scope, that folder will be scanned by the task.

4. If necessary, you an add objects to the scan scope:

   a. Click **Add**.

   b. In the **Add scan scope** window that opens, select a scope, an individual disk, a folder, or a network location.

      When a local hard drive is added to the scan scope, Portable Auditor does not scan shared folders linked to it. If you want to include shared folders, you need to add them separately.

   c. Click **OK**.

      The added object will be displayed in the list.

d. Repeat steps a-d for each object you add.

Added objects are included in the scan scope by default. If necessary, exclude the item from the scan scope using the check box to the left of its name.

e. If necessary, remove an object from the scan scope by clicking the **Delete** button.

f. If necessary, you can edit an existing scan scope object by clicking the **Edit** button.

5. For each scan scope object, you can separately configure the *Malware Scan* task settings:

a. Select the scan scope object for which you want to configure the task settings, and click the **Scope settings** button.

b. The **Scope settings** window opens on the **General** tab.

c. Under **Action to perform on detected objects**, select the action that Portable Auditor will perform on infected and other detected objects:

- **Disinfect, delete if disinfection fails**. If this option is selected, the application automatically attempts to disinfect all infected files that are detected. If disinfection fails, the application deletes the files.
- **Inform** (default value). If this action is selected, Portable Auditor does not perform any actions on an infected object or other detected objects. The application only logs an event in the report. You can use this option for a quick scan or, for example, to scan systems in which industrial software modules must never be deleted.

d. In the **Scan objects** section, select the objects that you want to include in the scan scope:

- **All objects**. Portable Auditor scans all objects.
- **Objects scanned by format**. Portable Auditor scans only infectable objects based on file format. Formats are added to the list by Kaspersky experts; the list is part of the databases of Kaspersky Industrial CyberSecurity for Nodes.
- **Objects scanned by the list of extensions specified in anti-virus databases**. Portable Auditor scans only infectable objects based on file extension. Extensions are added to the list by Kaspersky experts; the list is part of the databases of Kaspersky Industrial CyberSecurity for Nodes.
- **Objects scanned by specified list of extensions**. Portable Auditor scans only infectable objects based on file extension. You can create your own list of extensions by clicking **Browse**.

e. In the **Scan of compound objects** section, specify the types of compound objects that you want to include in the scan scope:

- **Archives**. Scanning of ZIP, CAB, RAR, and ARJ archives and other archive formats.
- **SFX archives**. Scanning of self-extracting archives.
- **Packed objects**. Scanning of executable files packed by binary code packers, such as UPX or ASPack.
- **Plain email**. Scanning of files in mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

- **Email databases**. Scanning of Microsoft Outlook and Microsoft Outlook Express mail database files. This option is available if the **Plain email** check box is selected.

- **Embedded OLE objects**. Scanning of objects embedded in files (such as Microsoft Word macros, or email message attachments).

f. If the **Disinfect, delete if disinfection fails** option is selected, configure the **Entirely remove the compound file that cannot be modified by the application in case of embedded object detection** functionality. If this functionality is enabled, Portable Auditor forces the deletion of the entire parent compound object whenever a malicious or other nested object is detected. The parent file along with all of its contents are forcibly removed if the application cannot remove only the detected child object (for example, if the parent object cannot be modified). If this functionality is disabled, Portable Auditor does not delete the parent object. This option is enabled by default.

g. Go to the **Additional** tab.

h. You can make the scan finish sooner and increase the speed of Portable Auditor using settings under **Scan optimization**:

- **Stop scanning if it takes longer than (sec)**. If this functionality is enabled and it takes too long to scan an object, Portable Auditor will stop scanning that object and continue scanning the area. You can use this option, for example, if Portable Auditor takes too long to scan large files or the network environment. This option is enabled by default. Accepts values from 1 to 6000 seconds. The default value is 60 seconds.

- **Do not scan compound objects larger than (MB)**. If this option is enabled, Portable Auditor excludes from scanning objects that are larger than the specified size. This option is enabled by default. Available values: from 1 to 10 000 MB. The default value is 100 MB.

- **Use iChecker Technology**. This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scans by using a special algorithm that takes into account the release date of Portable Auditor databases, the date when the file was last scanned, and any modifications to the scan settings. There are limitations to iChecker Technology: it does not work with large files and applies only to files with a structure that the application recognizes (for example, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, and RAR).

i. Under **Scan exclusions**, if necessary, add exclusions from the scan scope:

- **Exclude files**. Use this functionality to exclude the files from scan scope and not remove them if detected. You can both specify a full file path and use a mask. By default, the functionality is disabled.

- **Do not detect objects by type**. You can use this feature to prevent the detection and subsequent deletion of objects of a certain type. You can specify the object name or use a mask. By default, the functionality is disabled.

6. If necessary, you can transfer custom task settings from one scan scope object to another:

a. Select the scan scope whose settings you want to transfer.

b. Click **Duplicate settings**.

c. This opens a window; in that window, select the scan scopes to which you want to apply the settings.

d. Click **OK**.

The task settings are transferred to the selected scopes.

7. To create scan exclusions, go to the **Exclusions** tab.

   Portable Auditor does not scan folders and objects from the exclusion list, even if they are included in the scan scope. For example, if a hard drive is added to the list of exclusions, Portable Auditor will not scan the folders included in the scan scope located on that drive.

8. Create scan exclusions:

   a. Click **Add**.

   b. This opens a window; in that window, select how you want to specify the exclusion:

   - **Exclude the category**. You can use this option to prevent the detection and subsequent deletion of objects of a certain type.
   - **Specify a path to the object**. Use this option to exclude the files from scan scope and not remove them if detected. You can both specify a full file path and use a mask.

   c. Click **OK**.

   d. Repeat steps a–c for all exclusions that you want to add.

9. Go to the **General settings** tab.

10. In the **Scan objects** section, specify object types that you want to include in the scan scope:

    - **Scan disk boot sectors**. If the functionality is enabled, Portable Auditor scans boot sectors and master boot records on hard drives and removable drives of the protected device. This option is enabled by default.
    - **Scan alternate NTFS streams**. Scanning of alternative file and folder streams on drives with the NTFS file system. If the functionality is enabled, Portable Auditor scans a potentially infected object and all NTFS streams associated with that object. If the functionality is enabled, the application scans only the object that was detected and considered as probably infected. This option is enabled by default.

11. Under **Consumption of computer resources**, if necessary, enable the **Limit CPU usage for scan tasks** functionality. If enabled, Portable Auditor limits the CPU usage on the scanned device by scan tasks. By default, the functionality is disabled.

    If enabled, manage the **Upper limit** setting. Range of available values: 10–100%. The default value is 50%

Security Audit task settings

To configure the Security Audit task:

1. In the **Security Audit** block, click the **Settings** button.

   The **Security Audit settings** window opens.

2. In the **Settings** field, select **Custom**.

3. Select the OVAL and XCCDF rule sources that Portable Auditor will use to audit device security:

   - **Kaspersky ICS CERT vulnerabilities database for SCADA**. Portable Auditor scans the device for all vulnerabilities described in the OVAL rules, in the Kaspersky ICS CERT for ICS vulnerability database. By default, the option is selected.
   - **Rules for collecting host configuration data**. Portable Auditor gathers information about the device configuration. By default, the option is selected.
   - **Compliance and security configurations for operating systems**. Portable Auditor checks the operating system settings of the device for compliance with security benchmarks. By default, the option is selected.

     It is not always known in advance which operating systems are installed on the scanned devices, so configurations for all supported operating systems are selected by default. If necessary, you can exclude unused configurations by clicking **Select configurations**.

     > Kaspersky ICS CERT vulnerabilities database for SCADA, Rules for collecting host configuration data, and Compliance and security configurations for operating systems are provided with the Portable Auditor databases. Therefore, before starting Portable Auditor with at least one of the listed rule sources, make sure that the Portable Auditor databases are up to date.

   - **Custom rule database**. Portable Auditor checks the device for vulnerabilities described in custom OVAL and XCCDF rules.

4. If the **Custom rule database** option is selected, download the rules databases:

   a. Click **Configure**.

   b. In the window that opens, specify a ZIP archive with the rule database.

   c. You can load only one archive containing an XML file with OVAL rules and XCCDF rules.

   d. Click **Open**.

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

Network traffic recording task settings

To configure the Network traffic recording task:

1. In the **Network traffic recording** block, click the **Settings** button.

   The **Network traffic recording settings** window opens.

2. In the **Settings** field, select **Custom**.

3. In the **Record inbound and outbound network traffic of the host being checked during the following time interval (sec)** field, change the period for Portable Auditor to record inbound and outbound traffic from the device being scanned. Range of available values: 1–1800 sec. The default value is 30 seconds.

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

Importing and exporting task settings

You can use the export/import functionality to transfer task settings from one instance of Portable Auditor to another.

To export task settings to a configuration file:

1. In the **Tasks** section, click the **Export settings** link.
2. In the window that opens, click the **Browse** button.
3. Enter the name of the XML file to which you want to export task settings, and select the folder for this file.
4. Click **Export**.

   Portable Auditor exports custom task settings, default task settings, and custom OVAL or XCCDF rules (if any) to an XML file.

To import task settings from a configuration file:

1. Go to the **Tasks** section.
2. Click the **Import settings** link.
3. In the window that opens, click the **Browse** button and select the XML file containing the Portable Auditor settings.
4. Click **Import**.

   The task settings from the file override the Portable Auditor custom task settings.

Viewing licensing information

To view the information about the current license,

In the Portable Auditor Console, go to the **Licensing** section.

General information about the current license is displayed in the results pane (see the table below).

General information about the license

Field	Description
Key status	Key status and license type
License key	The number of the key that you used to activate Portable Auditor.
Days left	The number of days remaining until the license expires.
Expiration date	License expiration date and time.
Activation date	Application activation date.

Color indication is additionally used for expiration notification in the **Licensing** section:

- *Red* means less than 10 days remain until the license expires.
- *Yellow* means 11 to 30 days remain until the license expires.
- *Green* means more than 30 days remain until the license expires.

After the license expires, you need to create Portable Auditor from scratch with a new key file.

Viewing the scan results

To view Portable Auditor task results:

1. Go to the **Reports** section.

   The results pane displays a table with a list of devices for which Portable Auditor stores task results.

2. You can export scan results:

   a. Select one or more devices for which you want to export scan results. You can select multiple devices by holding **CTRL** or **SHIFT** and clicking. To select all devices, press the **Select all** button.

   b. Click the **Export** button and select a folder for export.

   Portable Auditor exports the contents of the kavscan\Results\<Name of the scanned device> folder to the selected folder.

3. After export, you can delete files with scan results from the removable drive by clicking the **Clear** button.

4. To view task reports, select a device and click the **View** button.

5. This opens a window; in that window, click the name of the task for which you want to view the report.

   If the task was completed successfully, a report is displayed in the right part of the window:

   - For a *Malware Scan* task, a table with information about threats is displayed:
     - **Object name** is the name of the infected file.
     - **Threat name** is the threat name that is listed in the Kaspersky IT Encyclopedia.
     - **Object path** is the full path to the detected object on the scanned device.
     - **Scan time** is time when the object was detected.
     - **Reason** is the reason why the detected object was not detected by the application.

     You can export the task report using the **Export the Malware Scan task report** button. Portable Auditor exports a ZIP archive containing the report on detected threats and saves it in the specified folder.

   - For *Security Audit* and *Network traffic recording* tasks, reports cannot be viewed in the Portable Auditor Console. To view the results of these tasks, you need to export the reports by clicking the **Export** button.

Portable Auditor result files and their storage

The Portable Auditor results, written to the secure removable drive, are hidden. To gain access to the results of such a Portable Auditor, you must export these to any other available media in the Portable Auditor Console or on the command line.

After the scan is complete, a Results folder is created in the kavscan folder. It has the following structure:

- <scanned device name>: a folder named after the device being scanned and containing the following subfolders:
  - <date_time>: a folder whose name includes the date and time of the device scan in the format YYYY-MM-DD_HH-MM-SS. Depending on the scan settings, it may contain the following subfolders:
    - The Backup folder contains backup copies of the original files that the application tried to disinfect if the scan task was running in the **Disinfect, delete if disinfection fails** mode. Each file contains the path in its name, where the file was located on the scanned device. Each file is packed into a password-protected .ZIP archive. Use `infected` as a password to get access to the files.
    - Detects: a folder containing service information about detections. The contents of the folder are necessary for displaying alert details in Kaspersky Industrial CyberSecurity for Networks.
    - Oval: a folder containing a ZIP archive with an XML and HTML report for each source of audit security rules. The folder exists if a Security Audit has been performed.
    - Network: a folder containing dumps of inbound and outbound traffic from the device. The folder exists if the *Network traffic recording* task has been run.
    - The Report folder contains a report.txt file with the Portable Auditor report.
    - Results: a folder containing a results_<scanned device name>_<scan date_time>.zip archive with artifacts containing the results of the completed scan. This archive is necessary for importing scan results into Kaspersky Industrial CyberSecurity for Networks.
    - Temp: a folder containing temporary data created during the scan.

Viewing the general Portable Auditor report

After the tasks are complete, a report.txt file is created in kavscan\Results\<scanned device name>\<date_time>\Reports.

The report incorporates the following sections:

- **Title**
  - Portable Auditor version
  - Date and time when the scan was started

- Command used to start the scan
- Name of the device that initiated the scan
- Operating system of the scanned device
- Network interface: name, MAC address, IP address
- User that initiated the scan
- Date and time when the databases were created
- Date and time when the *Security Audit* task was performed
- Rule sources that Portable Auditor will use to audit device security
- Date and time when the *Security Audit* task was completed
- Date and time when the *Malware Scan* task was performed
- Scan scope

- **List of events**

  The list of events contains the scan details for the `/type=full` and `/type=critical` modes. It contains the name of scanned device and the action performed for the detected objects.
  For the `/type=short` mode, the list of events is not generated.

- **Statistics**

  This section of the report contains the date and time when the scan completed and the number of objects in the following categories:

  - Detected
  - Infected objects and other objects detected
  - Objects not disinfected
  - Objects not scanned
  - Processing errors
  - Objects disinfected
  - Objects deleted
  - Password-protected objects
  - Objects processed.
  - Date and time when the scan was completed

To configure the details of the general scan report:

1. In the Portable Auditor Console, go to the **Malfunction diagnosis** section.
2. In the **Report type** block, select the appropriate level of detail:
   - **Full**: a full scan report containing all event types
   - **Critical**: a scan report containing only critical events
   - **Short**: a scan report containing only general statistics but no events

Updating Portable Auditor databases

You can view the release date and time of the application databases in the **Update** section of the Portable Auditor Console.

To update Portable Auditor databases:

1. Download the updated application databases in one of the following ways:
   - Using the distribution points repositories.

     On a device with Kaspersky Industrial CyberSecurity for Nodes installed, create or configure the existing *Download updates to the repositories of distribution points* task for a device or a group of devices. For more details on configuring the task, refer to the Kaspersky Security Center Help. Start the task.

     The version of Kaspersky Industrial CyberSecurity for Nodes installed on the device must match or be higher than the version of Kaspersky Industrial CyberSecurity for Nodes that was used to create Portable Auditor. Otherwise, the updated application databases may not contain certain files required for Portable Auditor to run properly.

   - Using the Kaspersky Updater Utility.

     Download the latest application databases to a folder on the device using the Kaspersky Updater Utility. For detailed information about using Kaspersky Update Utility, refer to the Kaspersky Knowledge Base.
2. Connect the removable drive containing Portable Auditor to a device with the updated application databases.
3. Start Portable Auditor Console.
4. Go to the **Update** section.

5. Click **Select source and update**.

6. This opens a window; in that window, specify the folder with the application databases downloaded at step 1.

Portable Auditor updates the application databases in the Bases folder and checks the databases. You can view the status of the update task in the **Status** field. Task status is additionally indicated with color:

- *Red* means the update finished with an error.
- *Green* means the update was successful or an update has not been started since the Portable Auditor was created.

Configuring Portable Auditor tracing and memory dump recording

To configure tracing and dumping for Portable Auditor:

1. In the Portable Auditor Console, go to the **Malfunction diagnosis** section.

2. Under **Dump settings**, select the **Create a dump file** check box to enable dumping. By default, memory dump recording is disabled.

   Portable Auditor saves Portable Auditor Console dump files to the kavscan\Crash Dumps\Application Console Crash Dumps folder, and application dump files to the kavscan\Crash Dumps\Application Crash Dumps folder.

3. Under **Tracing settings**, select the **Enable tracing** check box to enable tracing of the Portable Auditor. By default, Portable Auditor operation tracing is disabled.

4. Change the verbosity level of the debug information if necessary:

   - **Normal** means the trace file saves messages about all errors, warnings, as well as information about normal operation of Portable Auditor (default).
   - **Important** means the trace file saves messages about all errors, warnings, and additional information.
   - **Detailed** means the trace file saves all information about the operation of Portable Auditor.

   Portable Auditor saves the Portable Auditor Console trace files to the kavscan\Traces\Application Console Traces folder, and the application trace files to the kavscan\Traces\Application Traces folder.

5. To export dump and trace files, click the **Export dump and trace files** button and, in the window that opens, select a folder for the export.

Working with the Portable Auditor Console using the command line

To start Portable Auditor:

1. Connect the removable drive containing Portable Auditor to the device you want to scan.
2. Start a command-line interpreter with local administrator permissions on the device.
3. Run the `cd /d` command (for example, `cd /d "E:\kavscan"`, where `E` is the letter of the removable drive) to change to the folder that contains the kavscan.exe file.
4. Do one of the following:

   - If you want to start Portable Auditor with the settings specified before recording Portable Auditor, run the following command:

     ```
     KAVSCAN SCAN
     ```

   - If you want to run Portable Auditor with options different from those specified when Portable Auditor was created, run the following command:

     ```
     KAVSCAN SCAN [/AV] [/TRAFFIC=<duration in seconds>] [/OVAL=<full path to ZIP archive with security audit rules>] [/MYCOMPUTER] [/FIXED] [/REMOVABLE] [/REMOTE] [/SHARED] [/MEMORY] [/STARTUP] [/DRIVE=<disk>] [/FOLDER=<full path to folder to scan>] [/FILE=<full path to file including name>] [/CURE=<yes|no>] [/TRACE=<important|normal|detailed>] [/DUMP] [/REPORT=<full|critical|short>] [/SETTINGS=<full path to file with custom settings>]
     ```

     If `?` characters are displayed in the command line instead of the dialog, it means that the encodings of the operating system and Kaspersky Industrial CyberSecurity for Nodes do not match. For the dialog to be displayed correctly, you must manage your operating system settings to select the language of applications that do not support Unicode. You need to select the language that is being used by Kaspersky Industrial CyberSecurity for Nodes.

     To view help for commands, run the `KAVSCAN HELP` command.

     All `KAVSCAN SCAN` switches, except for `/CURE`, `/TRACE`, `/DUMP`, and `/REPORT`, override any original Portable Auditor settings. For example, if the `KAVSCAN SCAN` switches `/AV`, `/TRAFFIC`, and `/OVAL` are specified in any combination or on their own, Portable Auditor performs only those actions defined by the specified keys, even if the original Portable Auditor settings include all actions.

5. If you are starting Portable Auditor from a secure removable drive, enter the administrator password that you set up when you first configured Portable Auditor.

Command options for starting Portable Auditor

Parameter	Description
`/AV`	Starts scanning for viruses and other threats.
`/TRAFFIC=<duration in seconds>`	Logs inbound and outbound traffic from a device being scanned during the specified time. Accepts values from 1 to 1800. If no logging duration is set in the command, Portable Auditor uses its default duration. If no value is specified in the Portable Auditor settings, the default value of 30 seconds is used.
`/OVAL=<full path to the ZIP archive containing security audit rules>`	Initiates a security audit task according to the rules inside the specified ZIP archive. The ZIP archive must contain an XML file with rules written in OVAL or a set of XML files with rules written in XCCDF. You need to provide the complete path to the ZIP file, including its name. If the full path to the ZIP archive containing the rules is not specified, Portable Auditor runs the security audit according to its original settings.
`/MYCOMPUTER`	Starts scanning the entire computer.
`/FIXED`	Starts scanning all local hard drives.
`/REMOVABLE`	Starts scanning all removable drives.
`/REMOTE`	Starts scanning all remote drives.
`/SHARED`	Starts scanning the shared folders.
`/MEMORY`	Starts scanning all memory processes.
`/STARTUP`	Starts scanning the startup objects.
`/DRIVE=<drive>`	Starts scanning all boot sectors and files on the specified drive.
`/FOLDER=<full path to the folder to be scanned>`	Starts scanning the specified folder. You cannot use a folder label template as a value for the parameter.
`/FILE=<full path to the file including its name>`	Starts scanning the specified file. You need to specify the complete path to the file, including its name.
`/CURE=<yes|no>`	Defines the scanning mode. The following values are available: • `yes`: scan and disinfect. If the parameter is not set, the mode configured in settings is applied. • `no`: scan in detection mode. If the parameter is not set, the mode configured in settings is applied.
`/TRACE=<important|normal|detailed>`	Enables tracing of Portable Auditor operations. • `important` means the trace file saves messages about all errors, warnings, and additional information. • `normal` means that the trace file records messages about all errors and warnings, as well as information about the normal operation of Portable Auditor. • `detailed` means that all information about Portable Auditor operations is saved in the trace file (default value).
`/DUMP`	Enables dump recording.
`/REPORT=<full|critical|short>`	Defines the type of report created in Kavscan\Report\report.txt after the scan completes. The following values are available: • `full`: a full scan report containing all event types • `critical`: a scan report containing only critical events • `short`: a scan report containing only general statistics but no events. By default, the `short` type is applied.
`/SETTINGS=<full path to the file containing custom settings>`	Applies custom settings from the file located at the full path that includes the file name. If no value is specified, Portable Auditor applies its original settings. These settings are located in Kavscan\settings.dat.

Return codes of the `KAVSCAN SCAN` command:

- `0` – command successfully executed.
- `1` means a general error occurred.

Exporting Portable Auditor results from a secure removable drive

If Portable Auditor is written to a secure removable drive, the Portable Auditor results displayed in the kavscan\Results folder are written to a hidden drive partition. Therefore, it is not possible to directly view, copy, or transfer the results generated by Portable Auditor to another medium.

To export Portable Auditor results from a secure removable drive:

1. Connect the secure removable drive to the device to which you want to export the results from Portable Auditor.

   Kaspersky Industrial CyberSecurity for Nodes blocks third-party processes from accessing secure removable drives. To export the results from Portable Auditor, use a device that does not have Kaspersky Industrial CyberSecurity for Nodes installed, or disable blocking.

2. Start a command-line interpreter with local administrator permissions on the device.
3. Run the `cd /d` command (for example, `cd /d "E:\kavscan"`, where `E` is the letter of the removable drive) to change to the folder that contains the kavscan.exe file.
4. Run the following command:

   ```
   KAVSCAN EXPORT /FOLDER=<full path to folder> [/CLEAN]
   ```

   Where:

   `/FOLDER=<full path to folder>` specifies the full path to the folder you want to copy the Portable Auditor results to. This can be a folder on the device, a removable drive connected to the device, or a network share.

   `/CLEAN` indicates that the Portable Auditor results must be deleted from the secure removable drive. The application will not delete the Portable Auditor results if it cannot access the export folder or if the files have not been copied to that folder.

5. When prompted, enter the administrator PIN you set up before creating Portable Auditor.

The Portable Auditor results displayed in kavscan\Results will be copied to the folder at the specified path, and the folder structure will be saved. Adding the `/CLEAN` parameter deletes the Portable Auditor results.

To update Portable Auditor databases:

1. Start a command-line interpreter with local administrator permissions on the device.
2. Run the `cd /d` command (for example, `cd /d "E:\kavscan"`, where `E` is the letter of the removable drive) to change to the folder that contains the kavscan.exe file.
3. Connect the removable drive containing Portable Auditor to the device where the folder with the database updates is located.

4. Run the following command:

```
KAVSCAN UPDATE /SOURCE=<full path to folder>
```

where `<full path to folder>` is a repository of distribution points or a local folder with downloaded application databases.

Portable Auditor will update the application databases located in the Bases folder and then run a database integrity check. The results of this check will be displayed as a message in the command-line interface.

Blocking access to secure removable drives

Kaspersky Industrial CyberSecurity for Nodes can block access to secure removable drives connected to a device on which the application is installed. If blocking is enabled, a user on the device can only create a Portable Auditor and run *Secure copying of application databases* and *Secure update of application databases*, tasks on the device; access to the protected removable drive using standard means of the operating system is blocked.

You can configure blocking access to protected removable drives on the command line.

Managing Kaspersky Industrial CyberSecurity for Nodes on the command line

You can manage and administer Kaspersky Industrial CyberSecurity for Nodes on the command line.

To manage Kaspersky Industrial CyberSecurity for Nodes on the command line:

1. On the device, run a command line interpreter (for example, cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the kavshell.exe file is located.

   Example

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
   ```

   You can also add the executable file path to the %PATH% system variable during the application installation phase and run the command without navigating to the application folder.

3. Use the following template to execute the command:

   ```
   KAVSHELL <command> [options]
   ```

   You can view the list of commands for managing the application by running the `KAVSHELL HELP` command. To read about the syntax of a specific command, enter `KAVSHELL HELP <command>`.

As a result, Kaspersky Industrial CyberSecurity for Nodes performs the specified action.

APPCONTROL. Importing Applications Launch Control rules

The `KAVSHELL APPCONTROL` command allows importing rules of the Applications Launch Control component from an XML file, and removing all rules from the rule list of the component. To generate an XML file with rules, you can use a local or group *Rule Generator for Applications Launch Control* task.

Command syntax

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Required argument. Importing Applications Launch Control rules from the specified XML file: • `/APPEND` adds all rules from the file to the rule list of the component. If a rule is already in the list, it will be duplicated. • `/REPLACE` replaces the entire existing rule list of the component with the rules from the file. • `/MERGE` merges the rules from the file with the existing rule list. If a rule is already in the list, it will not be duplicated. To remove all rules of the Applications Launch Control component, use `/CLEAR`.
`<path to XML file>`	Required if `/APPEND`, `/REPLACE`, and `/MERGE` are passed. Full path to the XML file with rules.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG. Configuring the Applications Launch Control component

The `KAVSHELL APPCONTROL /CONFIG` command lets you manage the settings of the Applications Launch Control component.

Command syntax

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/MODE: <applyrules|statistics>`	Optional argument. The Applications Launch Control component operating mode: • `applyrules`: Kaspersky Industrial CyberSecurity for Nodes controls the launch of applications using Applications Launch Control rules. • `statistics` (default value): Kaspersky Industrial CyberSecurity for Nodes allows the startup of all applications. In this mode, the application only records information about all application launches, the rules that apply to the launched applications, and the actions that would have been performed if the component was running in `applyrules` mode.
`/DLL:<no|yes>`	Optional argument. DDL loading monitoring: • `no` (default value): Kaspersky Industrial CyberSecurity for Nodes does not control the loading of DLL modules using Applications Launch Control rules. Loading of DLL modules is allowed. • `yes`: If this functionality is enabled, Kaspersky Industrial CyberSecurity for Nodes allows or denies the loading of DLL modules using Applications Launch Control rules.
`/SAVETOFILE:<path to XML file>`	Optional argument. Saving the list of Applications Launch Control rules to the specified XML file.

`/SDC`	Optional argument. Export the application distribution cache to an XML configuration file specified by the `/SAVETOFILE` option.
`/CLEARSDC`	Optional argument. Deleting software distribution cache.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE. Rule Generator for Applications Launch Control

You can use the `KAVSHELL APPCONTROL /GENERATE` command to manage the *Rule Generator for Applications Launch Control* task.

Command syntax

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`<path to folder>`	Required if `/SOURCE` is not passed. Path to a folder with executable files, MSI packages, and scripts. The task will create allow rules if files of the specified types and in the specified folders are launched.
`/SOURCE:<path to file with folders list>`	Required if `<path to folder>` is not passed. Path to a TXT file with a list of folders with executable files for which allowing rules will be automatically generated.
`/MASKS:<edms>`	Optional argument. Extensions of executable files for which allowing rules will be automatically generated. You can include files with the following extensions in the task scope: • `e` for EXE files • `d` for DLL files • `m` for MSI files • `s` for scripts
`/RUNAPP`	Optional argument. Create allow rules based on running applications.
`/RULES:<ch|cp|h>`	Optional argument. The criterion that the task will apply when creating Applications Launch Control allow rules: • `ch` to use the digital certificate. If the certificate is missing, use the SHA256 hash. • `cp` to use the digital certificate. If the certificate is missing, use the path to the executable file. • `h` to use the SHA256 hash.

`/STRONG`	Optional argument. Use of the subject and thumbprint of the file's digital certificate as a criterion for triggering the allowing rules for Applications Launch Control. Used together with the `/RULES:<ch|cp>` parameter.
`/USER:<user or group of users>`	Optional argument. Name of the user or group of users for which the rules will be applied.
`/EXPORT:<path to XML file>`	Optional argument. Path and name of the XML file to which you want to save the specified rules.
`/IMPORT:<a|r|m>`	Optional argument. Import generated rules into the list of Application Launch Control rules: • `a` adds all rules from the file to the rule list of the component. If a rule is already in the list, it will be duplicated. • `r` replaces the entire existing rule list of the component with the rules from the file. • `m` merges the rules from the file with the existing rule list. If a rule is already in the list, it will not be duplicated.
`/PREFIX:<prefix for rules names>`	Specifying a prefix for the names of Applications Launch Control allowing rules.
`/UNIQUE`	Adding information to the rules about the protected device, based on which the Applications Launch Control allowing rules are generated.
`/ADDPATH`	Add a path to an executable file to rules generated based on hashes.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG. Supporting AM-PPL technology

The `KAVSHELL CONFIG` command allows you to manage application process protection using AM-PPL technology.

For the command to work properly, you need to disable Self-Defense mechanism.

Command syntax

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PPL:<ON|OFF>`	Required argument. Enables or disables AM-PPL technology support: • `ON` – enable support for AM-PPL technology. • `OFF` – disable support for AM-PPL technology.

`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

CREATEPORTABLE. Creating Portable Auditor

The `KAVSHELL CREATEPORTABLE` command lets you create a Portable Auditor on a removable drive.

Command syntax

```
KAVSHELL CREATEPORTABLE /DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>
/LICENSE=<path to the license key file> [/TOKENPIN=<password> [/NEWTOKENPIN=<password>]] [/VERIFY] [/AV <settings
of the scan for viruses and other threatening programs>] [/TRAFFIC=<duration in seconds>] [/OVAL <settings of the
security audit task>]
```

Command options

Parameter	Description
`/DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>`	Required argument. Allows you to select the removable drive on which Portable Auditor will be created. If Portable Auditor is to be written to a Rutoken removable drive, you must enter a ten-digit serial number of the Rutoken drive. You can find the serial numbers of the Rutoken drives connected to the current device by running the `KAVSHELL TOKEN /ENUMERATE` command.
`/LICENSE=<path to the license key file>`	Required argument. Specifies the path to the key file that is necessary for creating Portable Auditor.
`/TOKENPIN=<password>`	Required argument if a Rutoken removable drive is used. Sets an administrator password for accessing the Rutoken drive.
`/NEWTOKENPIN=<password>`	Optional argument. Sets a new administrator password for accessing the Rutoken drive.
`/VERIFY`	Optional argument. Verifies Portable Auditor after it is written to the removable drive.
`/AV <settings of the scan for viruses and other threatening programs>`	Optional argument. At least one of the `/av`, `/oval`, or `/traffic` arguments must be specified. Scans for viruses and other threatening programs.
`/TRAFFIC=<duration in seconds>`	Optional argument. Records incoming and outgoing traffic for a device being scanned during the specified time. Accepts values from 1 to 1800. The default value is 30 seconds.
`/OVAL <settings of the security audit task>`	Optional argument. Enables the security audit task.
Settings of the scan for viruses and other threatening programs	

`<list of files>`	Space-delimited list of files, folders, network paths, or predefined scan scopes.
`/L=<path to file with a list of scan scopes>`	Path to file with a list of scan scopes. The file must be created manually and saved in TXT format. The file must be saved with UTF-8 encoding without BOM.
`/MEMORY`	Starts scanning all memory processes. This scan scope is enabled by default.
`/SHARED`	Starts scanning the shared folders.
`/STARTUP`	Starts scanning the startup objects. This scan scope is enabled by default.
`/REMDRIVES`	Starts scanning all removable drives.
`/NETDRIVES`	Network drives scan
`/FIXDRIVES`	Starts scanning all local hard drives. This scan scope is enabled by default.
`/MYCOMP`	Starts scanning the entire computer.
`/F<A|C|E>`	Objects that should be included in the scan scope: • `/FA`: Scan all objects. The application scans all files without exception (all formats and extensions). • `/FC`: Scan objects by format. The application scans only objects whose formats are included in the list of formats of infectable objects. • `/FE`: Scan objects by extension. The application scans only objects with extensions included into the list of extensions of infectable objects.
`/AI=<action>`	Action to be applied to a detected infected object. Possible values: • `DISINFDEL` – **Disinfect, delete if disinfection fails** • `REPORT` (default value) – **Inform**
`/E=ABMSPO`	Exclude the specified object types. Possible values: • `A`: ZIP, CAB, RAR, and ARJ archives and other archive formats. • `B`: Microsoft Outlook and Microsoft Outlook Express mail database files. • `M`: files in mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages. • `S`: self-extracting archives. • `P`: executable files packed by binary code packers, such as UPX or ASPack. • `O`: objects embedded in files (such as Microsoft Word macros, or email message attachments). You can specify several parameter values.
`/EM=<file mask>`	Files that match the file mask are excluded from the scan scope. For example: • The mask `*.exe` will include all paths to files that have the exe extension. • The mask `example*` will include all paths to files named EXAMPLE.
`/ET=<scan duration in seconds>`	Files that take longer to scan than the specified time limit (in seconds) are excluded from the scan scope. The default value is 60 seconds.
`/ES=<size in megabytes>`	Files that are larger than the specified size limit (in megabytes) are excluded from the scan scope. The default value is 100 MB.
`/NOICHECKER`	Disable iChecker. This option is enabled by default.
`/EXCLUDE=<list of exlusions>`	List of files, folders, or network paths that will be excluded from the scope of the scan task. You can specify multiple values separated by spaces.
`/W=<file path>`	Path and name of the scan log file.
Settings of the security audit task	

`/SOURCE=<kl|kl-compl|file>`	Specifies the source of rules required by the Security Audit. Possible parameter values: • `kl` (enabled by default) – Kaspersky ICS CERT vulnerability database included in the distribution kit. • `kl-compl` (enabled by default) – Security configurations and standards compliance for operating systems, which are included in the distribution kit. • `file` – Custom rule database from file.
`/PATH=<full path to ZIP archive with security audit rules>`	This parameter passes the path to the files with rules for the **Custom rule database** source (`/SOURCE=file`). Initiates a security audit task according to the rules inside the specified ZIP archive. The ZIP archive must contain an XML file with rules in the OVAL language. You need to provide the complete path to the ZIP file, including its name. OVAL rules must be saved in the UTF-8 encoding without BOM.
`/MODE=<all|exclude|include>`	This parameter defines the vulnerability scan mode. Possible parameter values: • `all` – scans all vulnerabilities listed in the source. • `exclude` – scans the vulnerabilities listed in the source, except for those specified by the `/DEFINITIONS` parameter. • `include` – scans the vulnerabilities specified by the `/DEFINITIONS` parameter. Used together with the `/SOURCE=kl` parameter.
`/DEFINITIONS=<vuln_type_01;...;vuln_type_N>`	Semicolon-separated list of vulnerability types that must be scanned or must be excluded from being scanned. For example: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. Used together with the `/MODE=include` or `/MODE=exclude` parameter.

Example:

```
KAVSHELL CREATEPORTABLE /DRIVE=E: /LICENSE=C:\0000000A.key /VERIFY /AV /l="C:\Documents and Settings\file.txt"
/ai=DISINFDEL
```

DEVCONTROL. Importing Device Control rules

The `KAVSHELL DEVCONTROL` command lets you import rules of the Device Control component from an XML file produced by the *Rule Generator for Device Control* command or remove all rules from the rule list of the component.

Command syntax

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Required argument. Importing Device Control rules from the specified XML file: • `/APPEND` adds all rules from the file to the rule list of the component. If a rule is already in the list, it will be duplicated. • `/REPLACE` replaces the entire existing rule list of the component with the rules from the file. • `/MERGE` merges the rules from the file with the existing rule list. If a rule is already in the list, it will not be duplicated. To remove all rules of the Device Control component, use `/CLEAR`.
`<path to XML file>`	Required if `/APPEND`, `/REPLACE`, and `/MERGE` are passed. Full path to the XML file with rules.

Parameter	Description
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP. Recording memory dumps

The `KAVSHELL DUMP` command lets you enable or disable memory dumping.

Command syntax

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/ON`	Enable dump file creation.
`/F:` `<dump_file_folder>`	Required argument. Sets the folder in which the dump files are saved.
`/SNAPSHOT`	Creates a memory dump of a running process with the specified ID. The dump file is saved to the folder specified by the `/F` option.
`/P:<process_ID>`	Required if `/SNAPSHOT` is passed. Sets a process ID. You can find out the process ID by using the `tasklist` command.
`/OFF`	Disable dump file creation.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EDR_EXPERT_ON_PREM. EDR Expert (on-premises) integration

You can use the `KAVSHELL EDR_EXPERT_ON_PREM` command to configure the Kaspersky Endpoint Detection and Response Expert (on-premises) integration.

Command syntax

```
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /MODE:<EDRKATA|ERDExpertOnPrem> /SERVERS:<address>:<port> [/PINNED-
CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the certificate file>]
[/CLIENT-PASSWORD:<password for the client certificate>] [/TIMEOUT:<server connection timeout, in seconds>]
[/SYNC-PERIOD":<synchronization period with the server, in minutes> [/EVENTS-SEND-PERIOD:<period of send events to
server, in seconds>] [/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or
0>] [/EVENTS-PER-HOUR:<events count limit: max events per hour>] [/MAX-PACKET-LENGTH:<Maximum number of event
packets transmitted within a transaction>] [/TELEMETRY-SERVERS:<address>:<port>] [/TELEMETRY-PINNED-CERTIFICATE:
<full path to the telemetry server TLS certificate file>] [/TELEMETRY-CLIENT-CERTIFICATE:<full path to the
telemetry certificate file>] [/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>] [/TELEMETRY-
TIMEOUT:<Telemetry server connection timeout, in seconds>] [/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>] [/PWD:<password>]
[/LOGIN:<user name>]
| /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
| /SHOW
```

Command options

Parameter	Description
`/<ENABLE|DISABLE|SHOW>`	Required argument. Enabling, disabling, or viewing the status of the integration of Kaspersky Industrial CyberSecurity for Nodes with the Endpoint Detection and Response Expert (on-premises) solution.
`/MODE:<EDRKATA|ERDExpertOnPrem>`	Required argument. Select a solution to integrate with: • `EDRKATA`: Kaspersky Anti Targeted Attack Platform. • `ERDExpertOnPrem`: Kaspersky Endpoint Detection and Response Expert (on-premises)
`/SERVERS:<address>:<port>`	Required argument. Response server address and the port for connecting to the server. You can specify multiple values separated by `;`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Optional argument. TLS certificate for establishing a trusted connection between Kaspersky Industrial CyberSecurity for Nodes and a response server.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	Optional argument. Allows you to add a *crypto-container*, a PFX file that stores an encrypted client certificate for protecting the connection between Kaspersky Industrial CyberSecurity for Nodes and a SIEM server.
`/CLIENT-PASSWORD:<password for the client certificate>`	Required if `/CLIENT-CERTIFICATE` is passed. Lets you specify a password for the crypto-container.
`/TIMEOUT:<server connection timeout, in seconds>`	Optional argument. Maximum response server response timeout in seconds. Range of available values: 1–3600 sec. The default value is 10 seconds.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	Optional argument. The interval between requests to the response server in minutes. Range of available values: 1–60min. The default value is 5 minutes.

`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	Optional argument. The maximum delay time when sending events to the response server. When the specified time expires, the application tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. Range of available values: 1–3600 sec. The default value is 30 seconds.
`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	Optional argument. Lets you limit the number of events being sent: • `1`: enabled. • `0`: disabled (default value). If the number of events exceeds the configured limits, the application stops sending events.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	Optional argument. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.
`/TELEMETRY-SERVERS:<address>:<port>`	Required argument. Address and port of the telemetry server. You can specify multiple values separated by `;`.
`/TELEMETRY-PINNED-CERTIFICATE:<full path to the telemetry server TLS certificate file>`	Optional argument. TLS certificate for establishing a trusted connection with the telemetry collection server.
`/TELEMETRY-CLIENT-CERTIFICATE:<full path to the telemetry certificate file>`	Optional argument. Allows you to add a *crypto-container* that stores an encrypted client certificate for protecting the connection between Kaspersky Industrial CyberSecurity for Nodes and the telemetry collection server.
`/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>`	Required if `/CLIENT-CERTIFICATE` is passed. Lets you specify a password for the crypto-container.
`/TELEMETRY-TIMEOUT:<Telemetry server connection timeout, in seconds>`	Optional argument. The maximum time to wait for a response from the telemetry collection server in seconds. Range of available values: 1–3600 sec. The default value is 10 seconds.
`/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>`	Optional argument. Send telemetry with IOA only: • `1`: enabled. • `0`: disabled (default value).
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000
/PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx
/PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRExpertOnPrem /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-
HOUR=3000 /telemetry-SERVERS:127.0.0.1:8080;telemetry.server.ru:8080 /telemetry-TIMEOUT=30 /PINNED-
CERTIFICATE:c:\user\certs\telemetry_cert.pfx /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /DISABLE /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /SHOW
```

EDRKATA. KATA Integration

The `KAVSHELL EDRKATA` command lets you configure the integration with the Kaspersky Anti Targeted Attack Platform solution.

Command syntax

```
KAVSHELL EDRKATA /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the certificate file>] [/CLIENT-PASSWORD:<password for the client certificate>] [/TIMEOUT:<server connection timeout, in seconds>] [/SYNC-PERIOD:<synchronization period with the server, in minutes> [/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>] [/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>] [/EVENTS-PER-HOUR:<events count limit: max events per hour>] [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<current password>] [/LOGIN:<user name>] | /SHOW
```

Command options

Parameter	Description
`/<ENABLE|DISABLE|SHOW>`	Required argument. Enable, disable, or view the status of integration of Kaspersky Industrial CyberSecurity for Nodes with the Kaspersky Anti Targeted Attack Platform solution.
`/SERVERS:<address>:<port>`	Required argument. KATA Central Node server address (IPv4, IPv6) and port. You can specify multiple values separated by `;`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Optional argument. TLS certificate for establishing a trusted connection between Kaspersky Industrial CyberSecurity for Nodes and the Central Node server.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	Optional argument. Allows you to add a *crypto-container*, a PFX file that stores an encrypted client certificate for protecting the connection between Kaspersky Industrial CyberSecurity for Nodes and the Central Node server.
`/CLIENT-PASSWORD:<password for the client certificate>`	Required if `/CLIENT-CERTIFICATE` is passed. Lets you specify a password for the crypto-container.
`/TIMEOUT:<server connection timeout, in seconds>`	Optional argument. The maximum time to wait for a response from the telemetry collection server in seconds. Range of available values: 1–3600 sec. The default value is 10 seconds.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	Optional argument. The interval between requests to the Central Node server in minutes. Range of available values: 1–60min. The default value is 5 minutes.
`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	Optional argument. The maximum delay time when sending events to the Central Node server. When the specified time expires, the application tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. Range of available values: 1–3600 sec. The default value is 30 seconds.
`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	Optional argument. Lets you limit the number of events being sent: • `1`: enabled. • `0`: disabled (default value). If the number of events exceeds the configured limits, the application stops sending events.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	Optional argument. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.

`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000 /PWD:p@ssw0rd
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL EDRKATA /DISABLE /PWD:p@ssw0rd
KAVSHELL EDRKATA /SHOW
```

EXITPOLICY. Disabling policy on the device

The `KAVSHELL EXITPOLICY` command disables the Kaspersky Security Center policy on the device. After disabling the policy, all Kaspersky Industrial CyberSecurity for Nodes settings become available for configuration, including the settings marked in the policy with a closed padlock (🔒).

Command syntax

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT. Exporting application settings

The `KAVSHELL EXPORT` command lets you export Kaspersky Industrial CyberSecurity for Nodes settings from a configuration file in XML format. You can save all application settings or only settings for individual components to a configuration file.

Command syntax

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

Command options

Parameter	Description
`<profile>`	Required argument. Enter the export settings profile name. A profile is a component, task, or functionality of Kaspersky Industrial CyberSecurity for Nodes. You can view the list of available profiles by running the `KAVSHELL EXPORT /?` command. To export all application settings, specify the `product` profile.
`<file name>`	Required argument. Specify the file name in XML format to export the profile settings. You can also specify the file path. Example: `C:\Test\settings.xml` • If only a file name is specified in the command, the application attempts to place the file in the installation folder of the application. If the Self-Defense mechanisms of the application are enabled, the export will fail because the application's self-protection blocks the creation of a new file in the application folder. To export application settings, specify the file path.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.
`/PWD: <password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.

Example

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET. Clearing iSwift base

Kaspersky Industrial CyberSecurity for Nodes can use the iSwift technology, which lets the application avoid rescanning files that have not been modified since the last scan. The `KAVSHELL FBRESET` command clears the database that stores information about scanned uninfected files. After the database is cleared, Kaspersky Industrial CyberSecurity for Nodes scans all files that it accesses for the first time.

Command syntax

```
KAVSHELL FBRESET
```

FIM /BASELINE. Baseline System Integrity Monitor

You can use the `KAVSHELL FIM /BASELINE` command to manage the *Baseline System Integrity Monitor* task.

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring
areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task
id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id
baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task
id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/CREATE`	Starting a new *Baseline System Integrity Monitor* task that will create a snapshot of the system state.
`/SCAN`	Run *Baseline System Integrity Monitor* tasks with the ID of the system snapshot or an alternate name of an existing task.
`/CLEAR`	Deleting baseline. Specify the ID of a system snapshot or the alternative name of the task that created the snapshot. If neither an alternate task name nor a snapshot ID is specified, the application deletes all snapshots.
`/EXPORT`	Export data of all snapshots or the snapshot specified using the `/BL` option to the specified folder in a TXT file.
`/SHOW`	Display data from all snapshots of system state or the snapshot specified by the `/BL` option.
`<monitoring scope>`	Required if /L is not specified. Sets the monitoring scope of the task. You can use `*` and `?` characters to enter a path mask.
`/L`	Required if `<monitoring scope>` is not specified. Allows you to specify the path to the TXT file containing the list of monitoring scopes.
`/MD5`	Optional argument. Cannot be used together with the `/SHA256` parameter. Sets the MD5 algorithm for calculating the checksum. The MD5 algorithm is used by default.
`/SHA256`	Optional argument. Cannot be used together with the `/MD5` parameter. Sets the SHA256 algorithm for calculating the checksum. The MD5 algorithm is used by default.
`/SF`	Optional argument. Includes all subfolders in the monitoring scope of the task. By default, subfolders are not included in the monitoring scope.
`/ALIAS:<existing task id>`	Required if `/BL` is not specified. Task alias. You can find out the task alias by using the `KAVSHELL FIM /BASELINE /SHOW` command.
`/BL:<id baseline>`	Required if `/ALIAS` is not specified. Sets the ID of the system snapshot. You can find out the baseline ID by using the `KAVSHELL FIM /BASELINE /SHOW` command.
`/PWD:<password>`	Optional argument. Password of the KL Admin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KL Admin password.

Example

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

HELP. Displaying command help

To display the list of all available Kaspersky Industrial CyberSecurity for Nodes commands, run one of the following commands:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

To display a description of a command and its syntax, run one of the following commands:

```
KAVSHELL HELP <command>
KAVSHELL <command> /?
```

Example

```
KAVSHELL HELP SCAN
```

IMPORT. Importing application settings

The `KAVSHELL IMPORT` command lets you import Kaspersky Industrial CyberSecurity for Nodes settings from a configuration file in XML format. A configuration file can be created using the `KAVSHELL EXPORT` command.

Command syntax

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`<file name>`	Required argument. Specify the full path to the XML file, including its name and extension, from which you want to import settings.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

Command return values:

- 0: The operation completed successfully.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -4: Object not found.
- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.
- -501: Operation successful, but an error or warning occurred during execution (for example, the application did not import the settings of some components).
- -502: Import file is missing or has an unrecognized format.
- -503: Incompatible settings (configuration file exported from a different application or a later and incompatible version of Kaspersky Industrial CyberSecurity for Nodes).

KICS. Kaspersky Industrial CyberSecurity for Networks Integration

You can use the `KAVSHELL KICS` command to configure integration with Kaspersky Industrial CyberSecurity for Networks:

1. To configure the Kaspersky Industrial CyberSecurity for Nodes integration with Kaspersky Industrial CyberSecurity for Networks via the TCP protocol, run the following command:

```
KAVSHELL KICS /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>]
[/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for the crypto-
container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request period>]
[/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:<maximum
number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:<subnet
IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] [/LOGIN:<user name>] [/PWD:<password>]
```

2. To configure the Kaspersky Industrial CyberSecurity for Nodes integration with Kaspersky Industrial CyberSecurity for Networks in MQTT publisher mode, run the following command:

```
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:<address>:<port> [/MQTT-USER:<login name for
authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at the MQTT broker>] [/LOGIN:
<user name>] [/PWD:<password>]
```

3. To configure the Kaspersky Industrial CyberSecurity for Nodes integration with Kaspersky Industrial CyberSecurity for Networks via the UDP protocol, run the following command:

```
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:<address>:<port> [/UDP-ENCRYPTION-DISABLE] [/UDP-
ENCRYPTION-ENABLE] [/UDP-ENCRYPTION-KEY:<full path to the encryption key>] [/UDP-ENCRYPTION-PASSWORD:<password
to the encryption key>]
```

4. To configure the Kaspersky Industrial CyberSecurity for Nodes integration as an MQTT subscriber, run the following command:

```
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for the crypto-container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request period>] [/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:<maximum number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:<subnet IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] /MQTT-SUBSCRIBER-ENABLE /MQTT-SERVER:<address>:<port> [/MQTT-USER:<login name for authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at the MQTT broker>] [/LOGIN:<user name>] [/PWD:<password>]
```

Command options

Parameter	Description
`/<ENABLE|DISABLE|SHOW>`	Required argument. Allows enabling, disabling, or viewing the status of the integration between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks.
`/SERVERS:<address>:<port>`	Required argument. Allows you to specify the address and port of the Kaspersky Industrial CyberSecurity for Networks server or the address of an MQTT publisher. Range of possible port values: 1–65535.
`/KICS-MODE:<TELEMETRY|MQTT-PUBLISHER|UDP-DATA-DIODE>`	Optional argument. Allows selecting the integration mode of the application with Kaspersky Industrial CyberSecurity for Networks. • `TELEMETRY` is the mode for sending telemetry directly to the Kaspersky Industrial CyberSecurity for Networks server via the TCP protocol. • `MQTT-PUBLISHER` is the mode to be used for sending telemetry to the MQTT broker server. • `UDP-DATA-DIODE` is the mode for sending telemetry via a data diode using the UDP protocol. The default value is `TELEMETRY`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Optional argument. Allows you to add a TLS certificate for connecting Kaspersky Industrial CyberSecurity for Nodes with the Kaspersky Industrial CyberSecurity for Networks server.
`/CLIENT-CERTIFICATE:<full path to the crypto-container>`	Optional argument. Allows you to add a *crypto-container* that stores an encrypted client certificate for protecting the connection between Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Networks server.
`/CLIENT-PASSWORD:<password for the crypto-container>`	Required if `/CLIENT-CERTIFICATE` is passed. Lets you specify a password for the crypto-container.
`/TIMEOUT:<maximum server response timeout>`	Optional argument. Lets you specify the maximum response timeout in seconds of the Kaspersky Industrial CyberSecurity for Networks server. When the timeout runs out, Kaspersky Industrial CyberSecurity for Nodes attempts to connect to another Industrial CyberSecurity for Networks server if there is more than one. Range of available values: 1–3600 sec. The default value is 30 seconds.
`/SYNC-PERIOD:<synchronization request period>`	Optional argument. Lets you specify the interval between requests to the Kaspersky Industrial CyberSecurity for Networks server in minutes. When Kaspersky Industrial CyberSecurity for Nodes is working as an MQTT publisher, this setting sets the interval between requests to the MQTT broker if the connection with the broker becomes lost. Range of available values: 1–60min. The default value is 1 minute.

`/EVENTS-SENT-PERIOD:<maximum delay when sending events>`	Optional argument. Lets you specify the maximum delay when sending events to the Kaspersky Industrial CyberSecurity for Networks server. When the specified time expires, the application tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. Range of available values: 1–3600 sec. The default value is 30 seconds. When using Kaspersky Industrial CyberSecurity for Nodes as an MQTT subscriber, we do not recommend configuring the receipt of telemetry from more than 250 Kaspersky Industrial CyberSecurity for Nodes devices configured as MQTT publishers if the minimum **`/EVENTS-SENT-PERIOD`** value of 1 second is specified in the settings of MQTT publishers. If the setting is 30 seconds or more, we do not recommend to configuring receiving of data from more than 1000 MQTT publishers.
`/EVENTS-LIMIT:<1|0>`	Optional argument. Lets you limit the number of events being sent. If the number of events exceeds the configured limits, the application stops sending events.
`/EVENTS-PER-HOUR:<maximum number of events per hour>`	Required if `/EVENTS-LIMIT:1` is passed. Lets you specify the maximum number of events to be sent per hour. Range of available values: 10–65535. The default setting is 3000 events per hour.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.
`/VIRTUAL-SPAN-ENABLE`	Optional argument. Enables the promiscuous mode of telemetry. By default, Kaspersky Industrial CyberSecurity for Nodes collects network traffic arriving at network interfaces of the computer and addressed to the computer on which the application is installed. In promiscuous mode, the application collects network traffic for network interfaces of the computer coming from all available subnets. The application uses the collected traffic to generate extended telemetry. Not all network adapters support the Promiscuous mode. Extended telemetry collection does not work on these network adapters.
`/VIRTUAL-SPAN-DISABLE`	Optional argument. Disables the promiscuous mode of telemetry.
`/VIRTUAL-SPAN-ADD-RULES:<IPv4 addresses of the computer's network interfaces>`	Optional argument. Lets you add subnets as addresses of the computer's network interfaces (the application identifies the corresponding subnets by the subnet mask of the network interface) or addresses of network interfaces with subnets in the IPv4 format. The application collects network traffic in promiscuous mode only for network interfaces configured for the specified subnets. For example: `/VIRTUAL-SPAN-ADD-RULES:198.51.100.0; 198.51.100.0/24`.
`/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>`	Optional argument. Lets you delete subnets with specified IDs. The list of added subnets and their IDs can be displayed using the `KAVSHELL KICS /SHOW` command.
`/MQTT-SUBSCRIBER-ENABLE`	Optional argument. Enables the MQTT subscriber mode for receiving telemetry from the data diode. By default, the MQTT subscriber mode is disabled.
`/MQTT-SUBSCRIBER-DISABLE`	Optional argument. Disables the MQTT subscriber mode.

`/MQTT-SERVER:<address>:<port>`	Required parameter if the `/KICS-MODE:MQTT-PUBLISHER` or `/MQTT-SUBSCRIBER:ENABLE` parameter is passed. Specifies the address and port of the MQTT broker. The default port for the MQTT broker is 1883.
`/MQTT-USER:<login>`	Required parameter of login and password authorization is configured on the MQTT broker. Specifies the login name for authorization at the MQTT broker.
`/MQTT-PASSWORD:<password>`	Required parameter of login and password authorization is configured on the MQTT broker. Specifies the password for authorization at the MQTT broker.
`/UDP-SERVER:<address>:<port>`	Required if `/KICS-MODE:UDP-DATA-DIODE` is passed. Allows you to specify the address and port of the Kaspersky Industrial CyberSecurity for Networks server.
`/UDP-ENCRYPTION-ENABLE`	Optional argument. Enables encryption for data transmitted via the UDP protocol.
`/UDP-ENCRYPTION-DISABLE`	Optional argument. Disables encryption for data transmitted via the UDP protocol.
`/UDP-ENCRYPTION-KEY:<full path to the encryption key>`	Required if `/UDP-ENCRYPTION-ENABLE` is passed. Allows you to specify the path to an encryption key file with the .PEM extension.
`/UDP-ENCRYPTION-PASSWORD: <password to the encryption key>`	Required if `/UDP-ENCRYPTION-ENABLE` is passed. Allows you to specify a password for the encryption key.

Example

```
KAVSHELL KICS /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL KICS /DISABLE /PWD:p@ssw0rd
KAVSHELL KICS /SHOW
KAVSHELL KICS /VIRTUAL-SPAN-ENABLE /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-REMOVE-RULES:1,2,3 /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-ADD-RULES:192.168.73.0/24;192.168.73.0/24 /PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd
/PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:123.4.5.6:8080 /MQTT-SUBSCRIBER-ENABLE /MQTT-
SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd /PWD:p@ssw0rd
KAVSHELL KICS /MQTT-SUBSCRIBER-DISABLE
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:1.2.3.4:1234 /UDP-ENCRYPTION-ENABLE /UDP-ENCRYPTION-
KEY:c:\user\username\123e4567-e89b-12d3-a456-426655440990.pem /UDP-ENCRYPTION-PASSWORD:p@ssw0rd
```

Command return values:

- 0: The command completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.

ISOLATION. Managing Network isolation

You can use the `KAVSHELL ISOLATION` command to manage device network isolation locally.

Command syntax

```
KAVSHELL ISOLATION [/DISABLE] [/SHOW] [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/DISABLE`	Required if `/SHOW` is not passed. Disabling device network isolation.
`/SHOW`	Required if `/DISABLE` is not passed. Outputs the current network isolation settings on the device to the console.
`/PWD:<password>`	Required option for the `KAVSHELL ISOLATION /DISABLE` command. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command return values:

- 0: The operation completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -6: wrong operation (for example, an attempt to disable the component when it is already disabled).
- -7: Service not registered
- -8: Automatic Service startup disabled.
- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.

KSN. Using KSN/KPSN

You can use the `KAVSHELL KSN` command to select a Kaspersky solution for determining the reputation of files or websites. Kaspersky Industrial CyberSecurity for Nodes supports the following infrastructure solutions for working with Kaspersky reputation databases:

- *Kaspersky Security Network (KSN)* is the solution that is used by most Kaspersky applications. KSN participants receive information from Kaspersky and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases.

- *Kaspersky Private Security Network (KPSN)* is a solution that enables users of computers hosting Kaspersky Industrial CyberSecurity for Nodes or other Kaspersky applications to obtain access to Kaspersky reputation databases, and to other statistical data without sending data to Kaspersky from their own computers. KPSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

  - Local workstations are not connected to the Internet.

  - Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

Command syntax

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/GLOBAL`	Switching to using Kaspersky Security Network.
`/PRIVATE <settings-file>`	Switching to using Kaspersky Private Security Network. Specify the name of the configuration file containing Kaspersky Private Security Network settings. This file has the .PKCS7 or .PEM extension.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE. Application activation

Kaspersky Industrial CyberSecurity for Nodes keys and activation codes can be managed using the `KAVSHELL LICENSE` command.

Command syntax

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
No options specified.	The command returns the following information about added keys: • Key. • License type (commercial). • Duration of the license associated with the key. • Key status (active or additional). If the status is *, the key was added as an additional key.
`/ADD:<key_file | activation code>`	Activating Kaspersky Industrial CyberSecurity for Nodes with a key file. If the application is already activated, the key will be added as a reserve one.
`/R`	If the `/R` option is passed, the activation code or key is added as a reserve code or key.
`/DEL:<license key serial number>`	Delete the specified key or activation code.
`/REFRESH:<license id>`	Update the status of the specified license.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command return values:

- 0: The operation completed successfully.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -4: Key with specified number not found.
- -5: Syntax error.
- -6: Invalid operation (key already added).
- -99: Unknown error.
- -301: License is invalid.
- -303: License is for a different application.

MDR. Configuring the Managed Detection and Response integration

The `KAVSHELL MDR` command lets you configure the integration of Kaspersky Industrial CyberSecurity for Nodes with the Managed Detection and Response solution.

Command syntax

```
KAVSHELL MDR /ENABLE /BLOB:<path to pkcs7> [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/BLOB:<path to pkcs7>] [/PWD:<password>] [/LOGIN:<user name>] | /SHOW
```

Command options

Parameter	Description
`MDR /<enable|disable|show>`	Required argument. Lets you enable, disable, or view the current settings of the Managed Detection and Response (Industrial CyberSecurity) component.
`/BLOB:<full path to the MDR configuration file>`	Required argument. Allows you to specify the path to the MDR configuration file.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL MDR /ENABLE /BLOB:C:\some\folder\blob.pkcs7 /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

NETWORKBLOCKING. Managing Network Blocking

The `KAVSHELL NETWORKBLOCKING` command lets you locally disable the blocking of network connections of the device. For more details on blocking connections, please refer to the Kaspersky Industrial CyberSecurity for Networks Help.

Command syntax

```
KAVSHELL NETWORKBLOCKING /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/DISABLE`	Required argument. Disables blocking of network connections of the device.

`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command return values:

- 0: The command completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -6: wrong operation (for example, an attempt to disable the component when it is already disabled).
- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.

OMSINFO. Creating a JSON file with information about the application

The `KAVSHELL OMSINFO` command lets you create a JSON file with information about the current status of the application and detected threats, which you can then upload to monitoring systems.

Command syntax

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

Command options

Parameter	Description
`<oms_info_json_file_name>`	Full path to the JSON file including its name and extension.

Example

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

PASSWORD. Password-protected access to Kaspersky Industrial CyberSecurity for Nodes functionality

The `KAVSHELL PASSWORD` command allows you to manage password-protected access to Kaspersky Industrial CyberSecurity for Nodes functionality. If this functionality is enabled, the application requests a user name and password when deleting, modifying, or recovering the application, and when performing actions on the command line that may lower the protection level of the device.

Command syntax

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/SET`	Enables the password prompt to confirm critical actions.

`/NEW:<new password>`	Required if `/SET` is passed.
	Sets a new password.
	When creating a password, you are recommended to meet the following conditions:
	• The password doesn't contain the account name or computer name.
	• The password is at least 8 characters long.
	• The password contains characters that match at least three of the following categories:
	  • Uppercase Latin letters (A-Z)
	  • Lowercase Latin letters (a-z)
	  • Numerals (0-9)
	  • Exclamation mark (!), dollar sign ($), pound sign (#) and percent sign (%)

`/RESET`	Disables the password prompt to confirm critical actions.
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

PATCHCOMPATIBILITYRESET. Removing a patch from the list of incompatible patches

The `KAVSHELL PATCHCOMPATIBILITYRESET` command lets you remove a patch with the specified GUID from the list of incompatible patches. You can specify multiple GUIDs separated by spaces.

Command syntax

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

Example

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

PERFANALYZER. Exporting Performance Analyzer task results

The `KAVSHELL PERFANALYZER` command lets you export the results of the *Performance Analyzer* task to a JSON file.

Command syntax

```
KAVSHELL PERFANALYZER /EXPORT:<path to destination directory> [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/EXPORT:<path to destination directory>`	Required argument. Specify the path to the folder to which you want to export the file with the .JSON extension.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL PERFANALYZER /EXPORT:C:\PerfAnalyzer
```

Command return values:

- 0: The command completed successfully.
- -2: Service not running.
- -4: Object not found.

- -5: Syntax error.
- -99: Unknown error.

PREVENTION. Execution prevention

The `KAVSHELL PREVENTION` command lets you manage execution prevention for objects.

Command syntax

```
KAVSHELL PREVENTION /SHOW | /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description

`/SHOW`	Required if `/DISABLE` is not specified.
	Viewing the current Execution prevention settings. Upon executing the command, you will get the following response:
	`prevention.enabled=true|false`
	`prevention.mode=audit|prevent`
	`prevention.rules`
	`id: <rule ID>`
	`target: script|process|document`
	`md5: <MD5 hash of the file>`
	`sha256: <SHA256 hash of the file>`
	`pattern: <path to the object>`
	`case-sensitive: true|false`

`/DISABLE`	Required if `/SHOW` is not specified. Disabling Execution prevention.
`/PWD:<password>`	Required option for the `KAVSHELL PREVENTION /DISABLE` command. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL PREVENTION /DISABLE /LOGIN:Admin /PWD:p@ssw0rd
```

Command return values:

- 0: The operation completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -6: wrong operation (for example, an attempt to disable the component when it is already disabled).
- -7: Service not registered
- -8: Automatic Service startup disabled.

- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.

REMOTEACCESS. Managing Application Console remote connection settings

The `KAVSHELL REMOTEACCESS` command lets you manage remote connection settings of the Application Console to the device with Kaspersky Industrial CyberSecurity for Nodes installed.

Command syntax

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

Command options

Parameter	Description
`/SET [UIPORT | UIKLPORT]`	Set the port number: • `UIPORT` is the port for connecting with Windows credentials. • `UIKLPORT` is the port for connecting manually created users with credentials.
`/PORT=<new_port>`	Required if `/SET` is passed. Port number. Range of possible values: 1–65535.
`/RESET UIKLPORT`	Close the port for connecting manually created users with credentials.
`/SHOW`	Output the current port numbers.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID. Resetting device ID

The `KAVSHELL RESETMDRMACHINEID` command lets you reset the device ID used by the Managed Detection and Response solution.

Command syntax

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

RESTORE. Restoring files

The `KAVSHELL RESTORE` command lets you restore files from Backup and quarantine.

Command syntax

```
KAVSHELL RESTORE <filename> [/REPLACE][/QUARANTINE][/BACKUP]/PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
`<file name>`	Required argument. Full path to the file being restored.
`/REPLACE`	Optional argument. Overwrite an existing file. If this option is not passed, the file is restored only if there is no conflict.
`/QUARANTINE`	Optional argument. Restore files from Quarantine.
`/BACKUP`	Optional argument. Restore a file from Backup (default value).
`/PWD:<password>`	Required argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command syntax

```
KAVSHELL RESTORE /REPLACE C:\\eicar.com
KAVSHELL RESTORE /QUARANTINE C:\\test\eicar.com /PWD=1234 /LOGIN=user
```

Command return values:

- 0: The operation completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -6: Invalid operation.

- -7: Service not registered
- -8: Automatic Service startup disabled.
- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.

ROLLBACK. Last update rollback

The `KAVSHELL ROLLBACK` command starts the *Last update rollback* task.

Command syntax

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL ROLLBACK
```

Command return values:

- 0: The operation completed successfully.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -99: Unknown error.
- -221: Backup copy of database not found or corrupted.
- -222: Backup copy of database corrupted.

RTP. Real-Time File Protection

The `KAVSHELL RTP` command lets you enable or disable the Real-Time File Protection component.

Command syntax

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`</START|/STOP>`	Enable or disable the Real-Time File Protection component: • `/START` enables the component. • `/STOP` disables the component.
`/PWD:<password>`	Required option for the `KAVSHELL RTP /STOP` command. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

SCAN. On-Demand Scan

You can use the `KAVSHELL SCAN` command to create and start the *On-Demand Scan* task. To start an existing On-Demand Scan task from the command line, use the `KAVSHELL TASK` command.

Command syntax

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Command options

Parameter	Description
`<scan_scope>`	Required argument. Space-delimited list of files, folders, network paths, or standard scan scopes. Standard scan scopes: • `/MEMORY` scans all memory processes. • `/SHARED` scans shared folders. • `/STARTUP` scans startup objects. • `/REMDRIVES` scans removable drives. • `/FIXDRIVES` scans all local hard drives. • `/MYCOMP` scans the entire computer. You can specify multiple values separated by spaces.

Parameter	Description
`/L:<file_name>`	Optional argument. Path to file with a list of scan scopes. The file must be created manually and saved in TXT format. The file must be saved with UTF-8 encoding without BOM.
`/F<A|C|E>`	Optional argument. Objects that should be included in the scan scope: • `/FA`: Scan all objects. The application scans all files without exception (all formats and extensions). • `/FC`: Scan objects by format. The application scans only objects whose formats are included in the list of formats of infectable objects. • `/FE`: Scan objects by extension. The application scans only objects with extensions included into the list of extensions of infectable objects.
`/NEWONLY`	Optional argument. Scan only new and modified files. If this argument is not passed, Kaspersky Industrial CyberSecurity for Nodes scans all objects.
`/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>`	Optional argument. The action that you want the application to perform on infected and other objects: • `DISINFECT`: Disinfect, inform if disinfection fails. • `DISINFDEL`: Disinfect, delete if disinfection fails. • `DELETE`: Delete. • `REPORT` (default value): Inform. • `AUTO`: Recommended.
`/AS:<QUARANTINE|DELETE|REPORT|AUTO>`	Optional argument. The action that you want the application to perform on infected objects: • `QUARANTINE`: Move to Quarantine. • `DELETE`: Delete. • `REPORT` (default value): Inform. • `AUTO`: Recommended.
`/E:<ABMSPO>`	Exclude the specified object types. Possible values: • `A`: ZIP, CAB, RAR, and ARJ archives and other archive formats. • `B`: Microsoft Outlook and Microsoft Outlook Express mail database files. • `M`: files in mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages. • `S`: self-extracting archives. • `P`: executable files packed by binary code packers, such as UPX or ASPack. • `O`: objects embedded in files (such as Microsoft Word macros, or email message attachments). You can specify several parameter values.
`/EM=<file mask>`	Files that match the file mask are excluded from the scan scope. For example: • The *.exe mask will include all paths to files that have the EXE extension. • The example* mask will include all paths to files named EXAMPLE.
`/ET=<scan duration in seconds>`	Files that take longer to scan than the specified time limit (in seconds) are excluded from the scan scope. The default value is 60 seconds.
`/ES=<size in megabytes>`	Files that are larger than the specified size limit (in megabytes) are excluded from the scan scope. The default value is 100 MB.
`/TZOFF`	Do not apply Trusted Zone exclusions.
`/NOICHECKER`	Disabling the use of iChecker (enabled by default).
`/NOISWIFT`	Disabling the use of iSwift (enabled by default).
`/NOCHECKMSSIGN`	Do not scan files that are digitally signed by Microsoft.

Parameter	Description
`/ANALYSERLEVEL`	Enable Heuristic Analyzer, configure analysis level. The following heuristic analysis levels are available: • `1`: light. • `2`: medium. • `3`: deep. If this argument is not passed, the application does not use Heuristic Analyzer.
`/EXCLUDE=<list of exlusion`	List of files, folders, or network paths that will be excluded from the scope of the scan task. You can specify multiple values separated by spaces.
`/W=<file path>`	Path and name of the task log file. Restarting the command with the same log settings will overwrite the existing log file.
`/ANSI`	Use the ANSI encoding for events written to the task log. The `/ANSI` parameter will not be applied if the `/W` parameter is not passed. If the `/ANSI` parameter is not specified, Unicode is used to generate the task log.
`/ALIAS:<alternate name>`	Assign a temporary name to the task that it can be referred by while running. For example, task statistics can be viewed using the `KAVSHELL TASK` command. The alternate task name must be unique among all alternate task names in the application. If this argument is not passed, the task name is assigned as follows: scan_<kavshell_pid>. For example: scan_1234.

Example

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Command return values:

- 0: Operation completed successfully (no threats detected).
- 1: Operation canceled.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -4: Object not found (file with the list of scan scopes not found).
- -5: Syntax error or scan scope not set.
- -80: Infected objects detected.
- -81: Probably infected objects detected.
- -82: Object processing errors during scan.
- -83: Unscanned objects detected.
- -84: Damaged objects detected.
- -85: Failed to create task log.
- -99: Unknown error.
- -301: License is invalid.

SCAN-IOC. IOC Scan

You can use the `KAVSHELL SCAN-IOC` command to configure and start the *IOC Scan* task.

Command syntax

```
KAVSHELL SCAN-IOC <full path to IOC file> [/PATH:<path to folder with IOC files>] [/PROCESS=no] [/HINT=<full path
to the executable file of the process|full path to file>]
[/REGISTRY=no] [/DNSENTRY=no] [/ARPENTRY=no] [/PORTS=no] [/SERVICES=no] [/SYSTEM=no] [/USERS=no] [/VOLUMES=no]
[/EVENTLOG=no] [/DATETIME=<event publication date>] [/CHANNELS=<list of channels>]
[/FILES=no] [/DRIVES=<all|system|critical|custom>] [/NETWORK=no] [/URL=no] [/EMAIL=no] [/ROUTE=no] [/RETRO]
[/DEPTH=<1-14>] [/EXCLUDES=<list of exclusions>] [/SCOPE=<configurable list of folders>]
```

Command options

Options	Description
`<full path to IOC file>`	full path to the IOC file with the ioc or xml extension that you want to use for the search. Required if `/PATH:<path to the folder with IOC files>` is not specified.
`/PATH:<path to the folder with IOC files>`	Path to the folder with IOC files that you want to use for scanning. Required if `<full path to IOC file>` is not specified.
`/PROCESS=no`	Optional argument. Disable process information analysis during the scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not analyze processes running on the computer when performing the scan. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes process data only if the ProcessItem IOC document is described in the IOC file that is provided for the scan.
`/HINT=<full path to the executable file of the process|full path to the file>`	Optional argument. This argument allows narrowing down the scope of analyzed data for scans using ProcessItem and FileItem IOC documents by specifying an individual file. You can pass the following as the value of this argument: • `<full path to executable file of the process (ProcessItem)>` – ProcessItem • `<full path to file>` – FileItem This argument can only be passed in conjunction with the `/PROCESS=yes` and `/FILES=yes` arguments.
`/REGISTRY=no`	Optional argument. This argument disables the analysis of registry keys (IOC document RegistryItem) during the IOC scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not analyze information about registry keys. If the IOC file contains RegistryItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes the registry only if the RegistryItem IOC document is described in the IOC file that is provided for the scan.
`/DNSENTRY=no`	Optional argument. This argument disables the analysis of local DNS cache records (IOC document DnsEntryItem) during the IOC scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not scan the local DNS cache. If the IOC file contains DnsEntryItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes scans local DNS cache only if the DnsEntryItem IOC document is described in the IOC file that is provided for the scan.

/ARPENTRY=no	Optional argument. This argument disables the analysis of local ARP table records (IOC document ArpEntryItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan the local ARP table. If the IOC file contains ArpEntryItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes scans the local ARP table only if the ArpEntryItem IOC document is described in the IOC file that is provided for the scan.
/PORTS=no	Optional argument. This argument disables the analysis of information about ports being listened on (IOC document PortItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan the table of active connections on the device. If the IOC file contains PortItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes scans the table of active connections only if the PortItem IOC document is described in the IOC file that is provided for the scan.
/SERVICES=no	Optional argument. This argument disables the analysis of information about services installed on the device (IOC document ServiceItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan the information about services installed on the device. If the IOC file contains ServiceItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes service information only if the ServiceItem IOC document is described in the IOC file that is provided for the scan.
/SYSTEM=no	Optional argument. This argument disables the analysis of information about the environment (IOC document SystemInfoItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not analyze information about the environment. If the IOC file contains SystemInfoItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes environment information only if the SystemInfoItem IOC document is described in the IOC file that is provided for the scan.
/USERS=no	Optional argument. This argument disables the analysis of information about users (IOC document UserItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not analyze information about users created in the system. If the IOC file contains UserItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes information about users created in the system only if the UserItem IOC document is described in the IOC file that is provided for the scan.
/VOLUMES=no	Optional argument. This argument disables the analysis of information about volumes (IOC document VolumeItem) during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan the information about volumes on the device. If the IOC file contains VolumeItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes volume information only if the VolumeItem IOC document is described in the IOC file that is provided for the scan.

`/EVENTLOG=no`	Optional argument. This argument disables the analysis of Windows Event Log records (IOC document EventLogItem) during the IOC scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not scan Windows Event Log records. If the IOC file contains EventLogItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes Windows Event Log records only if the EventLogItem IOC document is described in the IOC file that is provided for the scan. For the EventLogItem\source IOC term, use the Provider Name value from the XML schema of the event.
`/DATETIME=<event publication date>`	Optional argument. The parameter allows enabling or disabling the consideration the date when the event was published in the Windows event log when determining the IOC scan scope for the corresponding IOC document. When performing an IOC scan, Kaspersky Industrial CyberSecurity for Nodes scans only those events that were published during the period from the specified time and date to the moment when the task is run. Kaspersky Industrial CyberSecurity for Nodes allows specifying the event publication date as the value of the argument. The scan is performed only for events published in the Windows event log after the specified date and before the scan is run. If the argument is not specified, Kaspersky Industrial CyberSecurity for Nodes scans events with any publication date. The setting is used only if the EventLogItem IOC document is described in the IOC file provided for the scan.
`/CHANNELS=<list of channels>`	Optional argument. This argument lets you pass a list of channel (log) names for which you want to perform an IOC scan. If this argument is passed, when running the IOC scan task, Kaspersky Industrial CyberSecurity for Nodes considers only events that have been published in the specified logs. The name of the log is specified as a string in accordance with the name of the log (channel) specified in the properties of the log (the Full Name parameter) or in the event properties (the <Channel></Channel> parameter in the xml schema of the event). By default (including the case when this argument is not passed), the IOC scan is performed for the Application, System and Security channels. You can pass multiple values in this argument (space-separated). The setting is used only if the EventLogItem IOC document is described in the IOC file provided for the scan.
`/FILES=no`	Optional argument. This argument disables the analysis of information about files (IOC document FileItem) during the IOC scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not analyze information about files. If the IOC file contains FileItem IOC document terms, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes file information only if the FileItem IOC document is described in the IOC file that is provided for the scan.
`/DRIVES=<all|system|critical|custom>`	Optional argument. This argument lets you specify the IOC scan scope when analyzing data for the FileItem IOC document. You can use one of the following values: • `all` makes the application scan all available file areas. • `system` makes the application scan only the files in folders in which the operating system is installed. • `critical` makes the application scan only temporary files in user and system folders. • `custom` makes the application scan only files in user-specified scopes. If the argument is not specified, critical areas are scanned.

`/NETWORK=no`	Optional argument. This argument disables the scan for threats based on the Network IOC document during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan for threats based on the Network IOC document. If the IOC file contains terms of the Network IOC document, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes enables the scan for threats based on the Network IOC document only if the Network IOC document is described in the IOC file that is provided for the scan.
`/URL=no`	Optional argument. This argument disables the scan for threats based on the UrlHistoryItem IOC document during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan for threats based on the UrlHistoryItem IOC document. If the IOC file contains terms of the UrlHistoryItem IOC document, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes enables the scan for threats based on the UrlHistoryItem IOC document only if the UrlHistoryItem IOC document is described in the IOC file that is provided for the scan.
`/EMAIL=no`	Optional argument. This argument disables the analysis of mail objects (IOC document Email) during the IOC scan. If the value of the argument is `<no>`, Kaspersky Industrial CyberSecurity for Nodes does not analyze mail objects. If the IOC file contains terms of the Email IOC document, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes analyzes mail objects only if the Email IOC document is described in the IOC file that is provided for the scan.
`/ROUTE=no`	Optional argument. This argument enables the scan for threats based on the RouteEntryItem IOC document during the IOC scan. If the value of the argument is <no>, Kaspersky Industrial CyberSecurity for Nodes does not scan for threats based on the RouteEntryItem IOC document. If the IOC file contains terms of the UrlHistoryItem IOC document, they are ignored (detected as no match). If this argument is not specified, Kaspersky Industrial CyberSecurity for Nodes enables the scan for threats based on the RouteEntryItem IOC document only if the RouteEntryItem IOC document is described in the IOC file that is provided for the scan.
`/RETRO`	Optional argument. This argument runs the task in *Retrospective IOC Scan* mode. With `/DEPTH=<interval in days>`, you can additionally pass the period for which you want the application to perform a retrospective IOC scan. The maximum value is 14 days. Time is counted from the moment when the task was started. Example: `KAVSHELL SCAN-IOC /PATH=<path to a folder with IOC files> /RETRO /DEPTH=2` If the time interval is not passed it defaults to 1 day.
`/EXCLUDES=<list of exclusions>`	Optional argument. This argument lets you specify exclusion scopes when analyzing data for the FileItem IOC document. You can pass multiple space-delimited paths in this argument. If the argument is not specified, the scan is performed without exclusions.
`/SCOPE=<configurable list of folders>`	Optional argument. This arguments becomes required if the `/DRIVES=custom` argument is specified. This argument lets you specify a list of scan scopes. You can pass multiple space-delimited paths in this argument.

If the command has completed successfully (return value `0`) and it detected indicators of compromise, Kaspersky Industrial CyberSecurity for Nodes outputs the following task result information to the command line:

Information that the application outputs to the command line when it detects indicators of compromise

`Uuid`	ID of the IOC file from the header of the IOC file structure (the `<ioc id="">` tag)
`Name`	Description of the IOC file from the header of the IOC file structure (the `<description></description>` tag)

`Matched Indicator Items`	List of IDs of all matched indicators.
`Matched objects`	Data for each IOC document for which there was a match.
`Date`	Creation date of the file in which indicators of compromise were found.
`Created`	Only for FileItem. Creation date of the object in which indicators of compromise were found.
`Pid`	ID of the process for which indicators of compromise were found.
`Upid`	Unique ID of the process for which indicators of compromise were found.
`ParentPid`	ID of the parent object containing the process for which indicators of compromise were found.
`Username`	Name of the user that modified the scanned object.
`StartTime`	Start time of the process for which indicators of compromise were found.

SCAN-OVAL. Security Audit

You can use the `KAVSHELL SCAN-OVAL` command to configure and start the *Security Audit* task. For the following rule sources, you can configure and launch a Security Audit task using the command line interface:

- **Kaspersky ICS CERT vulnerabilities database for SCADA**
- **Compliance and security configurations for operating systems**
- **Custom rule base from file**.

Command syntax

```
KAVSHELL SCAN-OVAL [/SOURCE:<kl|kl-compl|file>] [/REPOSITORY:show] [/PATH:<full path to the folder>] [/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>] [/MODE:<all|exclude|include>] [/DEFINITIONS:<vuln_type_01;...;vuln_type_N>] /RESULT-PATH:<path to the folder with the report> [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/SOURCE:<kl|kl-compl|file>`	Optional argument. Source of rules required by the Security Audit: • `kl` – Kaspersky ICS CERT vulnerability database included in the distribution kit. Available from the command line after successfully updating the Kaspersky Industrial CyberSecurity for Nodes databases and modules. • `kl-compl` – Security configurations and standards compliance for operating systems, which are included in the distribution kit. Available from the command line after successfully updating the Kaspersky Industrial CyberSecurity for Nodes databases and modules. • `file` – Custom rule database from file. If no parameter value is specified, the following source is used by default: **Kaspersky ICS CERT vulnerabilities database for SCADA** (`/SOURCE=kl`).
`/REPOSITORY:show`	Optional argument. This parameter is available if the selected rule source is security configurations and standards compliance for operating systems (`/SOURCE=kl-compl`). If the parameter is specified, then instead of executing the Security Audit task, Kaspersky Industrial CyberSecurity for Nodes saves an XML file that lists the names of the existing security configurations to the folder specified by the `/RESULT-PATH` parameter.

`/PATH:<full path to the folder>`	Optional argument. This parameter specifies the full path to the archive containing the XML file with OVAL rules, or to the archive containing XML files with OVAL and XCCDF rules for **Compliance and security configurations for operating systems** (`/SOURCE=kl-compl`) and **Custom rule base from file** (`/SOURCE=file`) sources. OVAL and XCCDF rules must be saved in UTF-8 without BOM.
`/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>`	Optional argument. This parameter specifies the full path and name of the ZIP archive with the XML file with external variables for OVAL rules. The parameter is available if the source contains only OVAL rules.
`/MODE:<all|exclude|include>`	Optional argument. This parameter defines the vulnerability scan mode. The parameter is available if the source contains only OVAL rules. Possible parameter values: • `all` – scans all vulnerabilities listed in the source. • `exclude` – scans the vulnerabilities listed in the source, except for those specified by the `/definitions` parameter. • `include` – scans the vulnerabilities specified by the `/definitions` parameter. If the parameter value is not specified, the `all` mode will be used by default.
`/DEFINITIONS: <vuln_type_01;...;vuln_type_N>`	Optional argument. Semicolon-separated list of vulnerability types that must be scanned or must be excluded from being scanned. The parameter is available if the source contains only OVAL rules. For example: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. Used together with the `/MODE=include` or `/MODE=exclude` parameter.
`/RESULT-PATH`	Required argument. Specifies the path to the folder where the scan report in XML format is stored. The file name contains the node name, as well as the date and time when the task was run. If the parameter is not specified, the task's execution will fail.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL SCAN-OVAL /SOURCE:kl /RESULT-PATH:c:\storage\reports
KAVSHELL SCAN-OVAL /SOURCE:kl-comp /REPOSITORY:show /RESULT-PATH:c:\storage\reports
```

SCANCRITICAL. Critical Areas Scan

The `KAVSHELL SCANCRITICAL` command starts the *Critical Areas Scan* task.

Command syntax

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/W`	Optional argument. Specify a file name with the .LOG extension for the exported task log. You can also specify the file path. If only a file name is specified in the command, the application attempts to place the file in the installation folder of the application. If the Self-Defense mechanisms of the application are enabled, the export will fail because the application's self-protection blocks the creation of a new file in the application folder. To export the log, specify the file path.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

SERVERBINDINGDISABLE. Disabling Administration Server connection protection

The `KAVSHELL SERVERBINDINGDISABLE` command locally disables the protection of the connection to the Administration Server. The command starts the *Administration Server connection protection* task, which removes the password of the computer's connection to the Administration Server.

Command syntax

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

SIEM. SIEM systems integration

The `KAVSHELL SIEM` command lets you configure the integration with SIEM systems for sending telemetry.

Command syntax

```
KAVSHELL SIEM /ENABLE /TLS /SERVERS=<protocol://server:port;protocol://server:port...> /TIMEOUT=<seconds> /PWD:
<password> /LOGIN:<user name> /PINNED-CERTIFICATE=<path> /CLIENT-CERTIFICATE=<path> /CLIENT-PASSWORD=<password>
/MAXIMUM-DATA-TRANSFER-TIME=<seconds> | /DISABLE | /SHOW
```

Command options

Parameter	Description
`/<ENABLE|DISABLE|SHOW>`	Required argument. Enable, disable, or viewing SIEM Integration component settings.
`/TLS`	Optional argument. Enable encryption of the connection between Kaspersky Industrial CyberSecurity for Nodes and SIEM servers.
`/SERVERS=<protocol://server:port;protocol://server:port...>`	Required argument. Specifies the server address and port. Range of possible port values: 1–65535.
`/TIMEOUT=<seconds>`	Optional argument. Maximum time to wait for a response from the SIEM server in seconds. Range of available values: 1–3600 sec. The default value is 30 seconds.
`/PINNED-CERTIFICATE=<path>`	Required if `/TLS` is passed. TLS certificate for establishing a trusted connection between Kaspersky Industrial CyberSecurity for Nodes and a SIEM server.
`/CLIENT-CERTIFICATE=<path>`	Optional argument. Allows you to add a *crypto-container*, a PFX file that stores an encrypted client certificate for protecting the connection between Kaspersky Industrial CyberSecurity for Nodes and a SIEM server.
`/CLIENT-PASSWORD=<password>`	Required if `/CLIENT-CERTIFICATE` is passed. Lets you specify a password for the crypto-container.
`/MAXIMUM-DATA-TRANSFER-TIME=<seconds>`	Maximum time to wait for a response from the SIEM server in seconds. When the specified time expires, Kaspersky Industrial CyberSecurity for Nodes tries to connect to the same server again or connects to the next server in the list, if there are multiple servers. Range of available values: 1–3600 sec. The default is 5 seconds.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL SIEM /ENABLE /SERVERS="tcp://server1:1234;udp://server2:5678;http://server3:9012" /TIMEOUT=10 /MAXIMUM-
DATA-TRANSFER-TIME=20"
```

```
KAVSHELL SIEM /DISABLE
KAVSHELL SIEM /SHOW
```

SIGMA. Anomaly Detection using Sigma rules

You can use the `KAVSHELL SIGMA` command to manage the Anomaly Detection using Sigma rules component.

Command syntax

```
KAVSHELL SIGMA /<ENABLE|DISABLE|ADD|REMOVE|SHOW> [/COLLECTION:<rat|deltav|uac|siemens|yokogawa|nfta|custom>]
[/NAME:<collection name>] [/SOURCE:<full path to the folder with the YAML files>] [/PWD:<password> [/LOGIN:<user
name>]
```

Command options

Parameter	Description
`/<ENABLE|DISABLE|ADD|REMOVE|SHOW>`	Required argument. Specifies one of the following actions: • `ENABLE` – enable Anomaly Detection using Sigma rules • `DISABLE` – disable Anomaly Detection using Sigma rules • `ADD` – add a collection of Sigma rules • `REMOVE` – remove a collection of Sigma rules • `SHOW` – display the current settings of Anomaly Detection using Sigma rules
`/COLLECTION:` `<rat|deltav|uac|siemens|yokogawa|nfta|custom>`	This parameter is required if `SIGMA /<ADD|REMOVE>` is specified. Specifies the type of Sigma rule collection to add or remove: • `rat`: Detection of remote administration tools (RAT). • `deltaV`: Anomaly detection for Emerson DeltaV. • `uac`: User account control (UAC). • `siemens`: Anomaly detection for Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7. • `yokogawa`: Anomaly detection for Yokogawa CENTUM VP. • `nfta`: Audit of file sharing over a network and via removable media. • `custom`: Custom rules collection. You can also specify `test`. One rule designed for internal testing at AO Kaspersky Lab is added or removed.
`/NAME:<collection name>`	This parameter is required if `SIGMA /<ADD|REMOVE>` and `/COLLECTION:custom` are specified. Specifies the name of a collection of custom Sigma rules.
`/SOURCE:<full path to the folder with the YAML files>`	This parameter is required if `SIGMA /ADD` and `/COLLECTION:custom` are specified. Specifies the full path to the folder with the YAML files that describe the custom Sigma rules.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.

Parameter	Description
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL SIGMA /ENABLE
KAVSHELL SIGMA /ADD /COLLECTION:deltav
KAVSHELL SIGMA /REMOVE /COLLECTION:custom /NAME:rules.yaml
```

START. Starting the application service

The `KAVSHELL START` command starts the Kaspersky Industrial CyberSecurity for Nodes Service service.

Command syntax

```
KAVSHELL START
```

STARTPOLICY. Enabling policy

The `KAVSHELL STARTPOLICY` command enables the Kaspersky Security Center policy on the protected device. The application settings will be configured according to the policy.

Command syntax

```
KAVSHELL STARTPOLICY
```

STOP. Stopping the application service

The `KAVSHELL STOP` command stops the Kaspersky Industrial CyberSecurity for Nodes Service service.

Command syntax

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.

`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KL Admin password.

Command return values:

- 0: The operation completed successfully.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -6: Invalid operation (the Kaspersky Industrial CyberSecurity for Nodes Service is already stopped).
- -7: Service not registered
- -8: Automatic Service startup disabled.
- -9: Attempt to run the managed device under a different user account failed.
- -99: Unknown error.

TASK. Managing tasks

You can use the `KAVSHELL TASK` command to manage Kaspersky Industrial CyberSecurity for Nodes tasks: run, pause, resume and stop the task and view the current task status and statistics.

Command syntax

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

Command options

Parameter	Description
No parameters	Return the list of all existing Kaspersky Industrial CyberSecurity for Nodes tasks. The list contains the following fields: the alternate name of the task (an additional brief name that Kaspersky Industrial CyberSecurity for Nodes for Windows assigns to tasks), the category of the task (system or user), and the current status of the task.
`<alternative name>`	Alternate name for the task that you want to manage. To view Kaspersky Industrial CyberSecurity for Nodes task aliases, enter the `KAVSHELL TASK` command without any parameters.
`/START`	Starting a task.
`/STOP`	Stopping a task.
`/STATE`	Display the current state of the task.
`/STATISTICS`	Display task statistics.
`/PWD:<password>`	Required option for the `KAVSHELL TASK /STOP` command. Password of the KL Admin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.

`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command syntax

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

Command return values:

- 0: The operation completed successfully.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -4: Object not found (task not found).
- -5: Syntax error or scan scope not set.
- -6: Invalid operation (for example, task not running, already running, or cannot be paused).
- -99: Unknown error.
- -301: License is invalid.
- 401: task not started (for the `KAVSHELL TASK <task name> /STATE` command).
- 402: task already started (for the `KAVSHELL TASK <task name> /STATE` command).
- 403: task paused (for the `KAVSHELL TASK <task name> /STATE` command).
- -404: Operation failed (a change in task status resulted in a crash).

TELEMETRYFILTERS. Exporting and importing telemetry event filtering rules

The `KAVSHELL TELEMETRYFILTERS` command lets you export or import rules for filtering telemetry events.

Command syntax

```
KAVSHELL TELEMETRYFILTERS [/IMPORT /EXPORT] <file_path> [/PWD:<password>] [/LOGIN:<user name>]
```

Command options

Parameter	Description
`/IMPORT <file_path>`	Required if `/EXPORT` is not passed. Import telemetry event filtering rules from a file. Specify the full path to the JSON file containing rules including its name and extension. If event filtering rules already exist on the computer, Kaspersky Industrial CyberSecurity for Nodes replaces these when importing.
`/EXPORT <file_path>`	Required if `/IMPORT` is not passed. Export telemetry event filtering rules to a JSON file. • If only a file name is specified in the command, the application attempts to place the file in the installation folder of the application. If the Self-Defense mechanisms of the application are enabled, the export will fail because the application's self-protection blocks the creation of a new file in the application folder. To export rules, specify the file path.
`/PWD: <password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL TELEMETRYFILTERS /IMPORT "C:\some\folder\telemetry_filers.json" /LOGIN:Admin /PWD:p@ssw0rd
```

TOKEN. Managing access blocking to secure removable drives

The `KAVSHELL TOKEN` command lets you manage the blocking of access to protected removable drives and also view information about protected removable drives connected to the device.

Command syntax

```
KAVSHELL TOKEN [/ENUMERATE | /PROTECTION:<status|enable|disable>]
```

Command options

Parameter	Description
`/ENUMERATE`	Lists the connected protected removable drives.
`/PROTECTION:<status|enable|disable>]`	Managing access blocking to secure removable drives: • `status` displays the current protection status. • `enable` enables protection. • `disable` disables protection.

Example

```
KAVSHELL TOKEN /ENUMERATE
KAVSHELL TOKEN /PROTECTION:status
KAVSHELL TOKEN /PROTECTION:enable
KAVSHELL TOKEN /PROTECTION:disable
```

TRACE. Tracing application operation

The `KAVSHELL TRACE` command lets you enable or disable tracing for the application.

Command syntax

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

Command options

Parameter	Description
`</ON | /OFF>`	Required argument. Enable or disable tracing for the application.
`/F:<traces_folder>`	Required if `/ON` is passed. Path to the folder in which the trace files will be saved.
`/S:<traces_size_in_MB>`	Optional argument. Maximum size of the trace file in megabytes. Available values: from 1 to 4095 MB. The default value is 100 MB.
`/LVL:` `<debug|info|warning|error|critical>`	Optional argument. Level of detail of debug information. • `critical` means the trace file saves only messages about fatal errors. • `error` means the trace file saves messages about all errors as well as warnings. • `warning` means the trace file saves messages about all errors, warnings, and additional information. • `info` (default value) means the trace file saves messages about all errors, warnings, as well as information about normal operation of the application. • `debug` means the trace file saves all information about the operation of the application.
`/R:<max trace files to rotate>`	Optional argument. Maximum number of files in a trace log. Available values: from 1 to 999. The default value is 5.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE. Updating databases and application software modules

You can use the `KAVSHELL UPDATE` command to manage the *Update* task.

Command syntax

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Command options

Parameter	Description
`<update_source | /AK | /KL>`	Required argument. Select update source: • `<update_source>` to use custom update sources. You can specify the path to a folder on the protected device, the path to a network folder in UNC format, or the address of an HTTP or FTP server on which the folder with updates is located. • `/AK` to use the Kaspersky Security Center Administration server as the update source. • `/KL` to use the Kaspersky update servers as the update source. You can specify multiple values separated by spaces.
`/NOUSEKL`	Optional argument. Do not use Kaspersky update servers if other update sources are not available (default value).
`/PROXY:<IP address>:<port>`	Optional argument. IP address or symbolic name of the proxy server and the port number.
`/AUTHTYPE:<0-2>`	Optional argument. Proxy server authentication type: • `0` for NTLM authentication with the current user account. • `1` for NTLM authentication with a user account whose user name and password are specified by the `/PROXYUSER` and `/PROXYPWD` options. • `2` for authentication with the user name and password specified by the `/PROXYUSER` and `/PROXYPWD` options.
`/PROXYUSER:<user_name>`	Required parameter if the `/AUTHTYPE:1` or `/AUTHTYPE:2` parameters are passed. User name that will be used to access the proxy server. If `/AUTHTYPE:0` is specified, then the `/PROXYUSER:<user_name>` and `/PROXYPWD:<password>` options are ignored.
`/PROXYPWD:<password>`	Required parameter if the `/AUTHTYPE:1` or `/AUTHTYPE:2` parameters are passed. User password that will be used to access the proxy server. If `/AUTHTYPE:0` is specified, then the `/PROXYUSER:<user_name>` and `/PROXYPWD:<password>` options are ignored. If the `/PROXYUSER` parameter is specified and the `/PROXYPWD` parameter is omitted, the password will be considered an empty string.
`/NOPROXYFORKL`	Optional argument. Do not use proxy server settings to connect to Kaspersky update servers.
`/USEPROXYFORCUSTOM`	Optional argument. Use proxy server settings to connect to user-defined update sources.
`/USEPROXYFORLOCAL`	Optional argument. Use proxy server settings to connect to local update sources.
`/NOFTPPASSIVE`	Optional argument. If this option is specified, Kaspersky Industrial CyberSecurity for Nodes uses the active mode for the FTP server connection. If this option is not passed, Kaspersky Industrial CyberSecurity for Nodes uses the passive connection mode, if possible.

`/TIMEOUT:<s>`	Optional argument. FTP or HTTP server connection timeout in seconds. Default value: 10 seconds.
`/REG:<code_by_iso3166>`	Optional argument. The code of the country in which the protected device is located, in accordance with the ISO 3166-1 standard. Example: `/REG:GR`. If this parameter is omitted or an invalid country code is specified, Kaspersky Industrial CyberSecurity for Nodes determines the location based on the regional settings of the protected device where the Application Console is installed. The application uses location information when selecting an update server.
`/W=<file path>`	Path and name of the task log file. Restarting the command with the same log settings will overwrite the existing log file.
`/ANSI`	Use the ANSI encoding for events written to the task log. The `/ANSI` parameter will not be applied if the `/W` parameter is not passed. If the `/ANSI` parameter is not specified, Unicode is used to generate the task log.
`/ALIAS:<alternate name>`	Assign a temporary name to the task that it can be referred by while running. For example, task statistics can be viewed using the `KAVSHELL TASK` command. The alternate task name must be unique among all alternate task names in the application. If this argument is not passed, the task name is assigned as follows: update_<kavshell_pid>. For example: update_1234.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Command syntax

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

Command return values:

- 0: The operation completed successfully.
- 200: All objects are up to date.
- -2: Service not running.
- -3: Insufficient permissions for running the command.
- -5: Syntax error.
- -99: Unknown error.
- -206: Extension files are missing in the specified source or have unknown format.
- -209: Error while connecting to the update source.
- -232: Authentication error while connecting to proxy server.

- -234: Kaspersky Security Center connection error.
- -235: Kaspersky Industrial CyberSecurity for Nodes was not authenticated when connecting to the update source.
- -236: Application databases are corrupted.
- -301: License is invalid.

YARA. Running YARA Scan

You can use the `KAVSHELL YARA` command to run a YARA Scan.

Command syntax

```
KAVSHELL YARA <full path to a YARA file> | /PATH=<path to a folder with YARA files> [<additional arguments>]
```

Command options

Required argument	Description
`<full path to a YARA file>`	Full path to the YARA file that you want to use for scanning. You can specify paths to multiple YARA files separated by spaces. Required if `/PATH` is not passed. Example: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/PATH=<path to a folder with YARA files>`	Full path to a folder with YARA files that you want to use for scanning. Required if `<full path to a YARA file>` is not passed. Example: `/PATH=C:\Users\Admin\Desktop\YARA`
`/FASTSCAN=<on|off>`	Optional argument. Quick YARA Scan. For each object, the application logs one occurrence of the detected indicator. The application also hides duplicates of detected indicators in the log. Quick YARA Scan allows scanning large files quicker. If this setting is not specified, the application performs a standard YARA scan. In this mode, the application reflects duplicates of detected indicators in the log.
`/MAXRULES=<maximum number of scan rules>`	Optional argument. Limit of the number of unique triggered rules that makes the application stop the YARA scan when reached. If the value of this setting is not specified or if `0` is specified, the application performs the YARA scan without limitations.
`/TIMEOUT=<N seconds>`	Optional argument. How long a YARA scan can take, in seconds. When this time runs out, the application stops the YARA scan. If the value of this setting is not specified or if `0` is specified, the application performs the YARA scan without limitations.
`/RECURSIVE=<on|off>`	Optional argument. This argument starts a recursive scan of subfolders within the `/SCANFOLDERS)` Custom Scan.
`/SCANFOLDERS=<path to folders for the YARA scan>`	Optional argument. This argument starts a YARA scan of files in the specified list of folders. You can specify multiple values separated by spaces. Kaspersky Industrial CyberSecurity for Nodes supports the `*` and `?` characters when entering a folder path mask. If this setting is not specified, the application performs a YARA scan of all local disks except network shares, cloud drives, and removable media.

`/SCANMEMORY=<on|off>`	Optional argument. Scan the memory of all running processes.
`/SCANPROCESS=<full paths to executable files of processes>`	Optional argument. Scan memory only for specified processes. Specify space-separated full paths to executable files of processes. You can also use `*` and `?` characters to enter a mask.
`/MAXSIZE=<size in bytes>`	Optional argument. Limit file size for the YARA scan. The application skips larger files.
`/INCLUDES=<list of objects for the YARA scan>`	Optional argument. Editing the scan scope. You can specify multiple values separated by spaces. The following values are available: • File name • File extension Scan scope must be specified with the `/SCANFOLDERS` parameter. Example: `/SCANFOLDERS C:\*.* /includes=*.exe *.dll` – the application scans all files with the .EXE and .DLL extensions on disk C.
`/EXCLUDES=<paths to objects to be excluded from the YARA scan>`	Optional argument. Excluding files from the YARA scan. You can specify multiple values separated by spaces. The following values are available: • File path • Mask of the file path Exclusions must be specified with the `/SCANFOLDERS` parameter. Example: `/SCANFOLDERS C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – the application skips the readme.txt file, all files from the C:\trusted folder, and all files with the .XML extension in the root folder on disk C.
`/SCANAUTORUNS=<on|off>`	Optional argument. YARA scan of autorun point objects.
`/EXCLUDEAUTORUNS=<list of autorun point objects to exclude from the YARA scan>`	Optional argument. Excluding autorun point objects from the scan scope. Specify space-separated full paths to executable files of processes. You can also use `*` and `?` characters to enter a mask.
`/LOGFOLDER=<path for saving scan results>`	Optional argument. If you specify a path to a folder, the application saves scan results at the specified path in a file named yara_<computer name>_<scan completion time>.txt. If you specify a path to a specific TXT file, the application saves the scan results in that file. For example: `/LOGFOLDER=C:\test` or `/LOGFOLDER=C:\test\abc.txt`. Scan results are output to the command line regardless of whether the `/LOGFOLDER` option is specified.
`/PWD:<password>`	Optional argument. Password of the KLAdmin user account or a user account with sufficient permissions. If this option is not specified, the application prompts you for the password on the next line.
`/LOGIN:<user name>`	Optional argument. User account name with sufficient permissions. If this option is not specified, the application prompts you for the user name on the next line. You do not need to enter this value if you entered the KLAdmin password.

Example

```
KAVSHELL YARA C:\rule.yara /SCANFOLDERS=c:\scanFolder\ /RECURSIVE=on
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ /FASTSCAN=on
KAVSHELL YARA c:\rules\rule1.yara c:\rules\rule2.yara /SCANFOLDERS=c:\scanFolder\ /LOGFOLDER=c:\yara_logs\
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ c:\scanFolder2\ /LOGFOLDER=c:\yara_logs\
```

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

How to get technical support

If you cannot find a solution to your problem in the documentation or in other sources of information about Kaspersky Industrial CyberSecurity for Nodes, we recommend that you contact Technical Support. Technical Support will answer your questions about installing and using Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky provides support for Kaspersky Industrial CyberSecurity for Nodes during the application's life cycle (refer to the application life cycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- By visiting the Technical Support website
- By sending a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. Kaspersky CompanyAccount is designed to facilitate interaction between users and Kaspersky specialists via online requests. Kaspersky CompanyAccount lets you monitor the progress of electronic request processing by Kaspersky specialists and store a history of electronic requests.

You can register all of your organization's employees under a single user account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian

- French
- Japanese

You can learn more about Kaspersky CompanyAccount on the Technical Support website.

Providing extended diagnostic information to Technical Support specialists

For more effective support and troubleshooting of application problems, Technical Support specialists may ask you to change application settings temporarily for purposes of debugging during diagnostics. This may require doing the following:

- Activating the functionality that processes and stores extended diagnostic information.
- Fine-tuning the settings of individual software components, which are not available via standard user interface elements.
- Changing the settings of storage and transmission of diagnostic information that was processed.
- Configuring the interception and logging of network traffic.

All information required to perform the listed actions (description of the sequence of steps, changeable settings, configuration files, scripts, additional command line features, debugging modules, specialized utilities, etc.), as well as the composition of data analyzed for debugging purposes, will be announced by the Technical Support specialists. The advanced diagnostic information is stored on the user computer. Automatic transfer of the stored data to Kaspersky is not performed.

After you report a problem to Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Industrial CyberSecurity for Nodes and to send it to Technical Support. Kaspersky Technical Support specialists may also ask you to create a trace file, send a memory dump file, and provide a report from the Kaspersky Get System Info utility.

After analyzing the data you send, Technical Support specialists can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

The actions listed above can only be performed under the guidance of the Technical Support specialists following the instructions received from them. Unassisted modification of the application settings in the ways not described in the application documentation or in the recommendations from the Technical Support specialists can lead to slowdowns and malfunctions of the operating system, decrease of the computer protection level, as well as to a violation of the availability and integrity of the processed information.

Tracing application operation

Application tracing is a detailed record of actions performed by the application and of messages about events that occur during operation of the application. During the tracing process, the application creates a set of files with data about the operation of different application components.

Application tracing should be performed under the supervision of Kaspersky Technical Support.

Trace files allow tracing the process of performing application commands step by step and determining the stage of application operation at which an error occurs.

How to enable and configure application tracing in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.
3. In the policy properties window, go to the **Malfunction diagnosis** section.
4. In the **Malfunction diagnosis settings** block, click the **Settings** button.

   The **Malfunction diagnosis settings** window opens on the **Application tracing settings** tab.
5. Use the **Enable tracing** check box to enable or disable tracing of application operation.

   By default, application operation tracing is disabled.
6. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, specify the full path to the local folder in the **Trace files folder** field.

   The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

   In the selected folder, Kaspersky Industrial CyberSecurity for Nodes creates a subfolder named logs-Kaspersky Industrial CyberSecurity for Nodes-<uid> to store trace files, where <uid> is a unique 8-character log identifier.
7. Select the level of detail of debug information:

   - **Normal** means the trace file saves messages about all errors, warnings, as well as information about normal operation of the application (default).
   - **Critical** means the trace file saves only messages about fatal errors.
   - **Diagnostic** means the trace file saves messages about all errors as well as warnings.
   - **Important** means the trace file saves messages about all errors, warnings, and additional information.
   - **Detailed** means the trace file saves all information about the operation of the application.

   A Technical Support representative determines the detail level required to resolve any potential issues.

8. To delete old trace files, enable the **Remove the oldest trace files** functionality.

   If this functionality is enabled, configure the maximum size and number of trace files:

   a. Specify the **Maximum size of a trace file (MB)**.

      Available values: from 1 to 4095 MB. The default value is 100 MB.

   b. Specify the **Maximum number of files for one trace log**.

      Available values: from 1 to 999. The default value is 5.

9. Save your changes.

How to enable and configure application tracing in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and do one of the following:

   - Click the **Application properties** link in the results pane of the node.
   - Select **Application properties** in the node's context menu.

   The **Application properties** window opens.

2. Select the **Malfunction diagnosis** tab.

3. In the **Malfunction diagnosis settings** block, click the **Settings** button.

   The **Malfunction diagnosis settings** window opens.

4. Select the tracing settings tab:

   - **Application tracing settings**. Kaspersky Industrial CyberSecurity for Nodes starts tracing for the application.
   - **Application Console tracing settings**. If Application Console and Kaspersky Industrial CyberSecurity for Nodes are installed on different computers, you can start tracing only for the Application Console.

5. Use the **Enable tracing** check box to enable or disable tracing of application operation.

   By default, application operation tracing is disabled.

6. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, click the **Browse** button and select the required folder.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

   In the selected folder, Kaspersky Industrial CyberSecurity for Nodes creates a subfolder named logs-Kaspersky Industrial CyberSecurity for Nodes-<uid> to store trace files, where <uid> is a unique 8-character log identifier.

7. Select the level of detail of debug information:

   - **Normal** means the trace file saves messages about all errors, warnings, as well as information about normal operation of the application (default).
   - **Critical** means the trace file saves only messages about fatal errors.

- **Diagnostic** means the trace file saves messages about all errors as well as warnings.
- **Important** means the trace file saves messages about all errors, warnings, and additional information.
- **Detailed** means the trace file saves all information about the operation of the application.

A Technical Support representative determines the detail level required to resolve any potential issues.

8. To delete old trace files, enable the **Remove the oldest trace files** functionality.

   If this functionality is enabled, configure the maximum size and number of trace files:

   a. Specify the **Maximum size of a trace file (MB)**.

      Available values: from 1 to 4095 MB. The default value is 100 MB.

   b. Specify the **Maximum number of files for one trace log**.

      Available values: from 1 to 999. The default value is 5.

9. Save your changes.

How to enable and configure application tracing in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management → Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Malfunction diagnosis** section.
5. In the **Malfunction diagnosis settings** block, use the **Enable application tracing** check box to enable or disable tracing of application operation.

   By default, application operation tracing is disabled.
6. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, specify the full path to the local folder in the **Traces folder (full path to folder, for example C:\\Traces\\)** field.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

   In the selected folder, Kaspersky Industrial CyberSecurity for Nodes creates a subfolder named logs-Kaspersky Industrial CyberSecurity for Nodes-<uid> to store trace files, where <uid> is a unique 8-character log identifier.
7. Select the level of detail of debug information:
   - **Normal** means the trace file saves messages about all errors, warnings, as well as information about normal operation of the application (default).
   - **Critical** means the trace file saves only messages about fatal errors.
   - **Diagnostic** means the trace file saves messages about all errors as well as warnings.

- **Important** means the trace file saves messages about all errors, warnings, and additional information.
- **Detailed** means the trace file saves all information about the operation of the application.

A Technical Support representative determines the detail level required to resolve any potential issues.

8. To delete old trace files, enable the **Remove older trace files** functionality.

   If this functionality is enabled, configure the maximum size and number of trace files:

   a. Specify the **Maximum size of trace files (MB)**.

      Available values: from 1 to 4095 MB. The default value is 100 MB.

   b. Specify the **Maximum number of files for one trace log**.

      Available values: from 1 to 999. The default value is 5.

9. Save your changes.

You can also enable and configure application tracing in the Compact Diagnostic Interface and on the command line.

Contents and storage of trace files

> You are personally responsible for the security of the data that is stored on your computer, particularly for monitoring and restricting access to the data until it is submitted to Kaspersky.

Trace files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed.

Trace files are stored in the following folder: %ProgramData%\Kaspersky Lab\KICS.5.0\Traces.

Trace files are named as follows: KICS<5.0_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.

You can view data saved in trace files.

All trace files contain the following common data:

- Event time
- Number of the thread of execution
- Application component that caused the event
- Degree of event severity (informational event, warning, critical event, error)
- A description of the event involving command execution by a component of the application and the result of execution of this command.

Contents of SRV.log, GUI.log, and ALL.log trace files

SRV.log, GUI.log and ALL.log trace files may store the following information in addition to general data:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on the local computer.
- The user name and password if they were transmitted openly. This data can be recorded in trace files during Internet traffic scanning.
- The user name and password if they are contained in HTTP headers.
- The name of the Microsoft Windows account if the account name is included in a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.
- Proxy server address, computer name, port, IP address, and user name used to sign in to the proxy server. This data is written to trace files if the application uses a proxy server.
- Remote IP addresses to which your computer established connections.
- Network traffic data. This data is written to trace files if traffic monitoring components are enabled.
- Data received from Kaspersky servers (such as the version of anti-virus databases).
- Statuses of Kaspersky Industrial CyberSecurity for Nodes components and their operating data.
- Data on user activity in the application.
- Operating system events.

Contents of HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log trace files

In addition to general data, the HST.log trace file contains information about the execution of a database and application module update task.

In addition to general data, the BL.log trace file contains information about events occurring during operation of the application, as well as data required to troubleshoot application errors. This file is created if the application is started with the avp.exe –bl parameter.

In addition to general data, the Dumpwriter.log trace file contains service information required for troubleshooting errors that occur when the application dump file is written.

In addition to general data, the WD.log trace file contains information about events occurring during operation of the avpsus service, including application module update events.

In addition to general data, the AVPCon.dll.log trace file contains information about events occurring during the operation of the Kaspersky Security Center connectivity module.

Contents of the AMSI Scanner component trace file

In addition to general data, the AMSI.log trace file contains information about the results of scans performed on requests from third-party applications.

Contents of trace files of the application web plug-in

Trace files of the application web plug-in are stored on the computer on which Kaspersky Security Center Web Console is deployed, in the folder Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

Trace files of the application web plug-in are named as follows: logs-kics_windows-<type of trace file>.DESKTOP-<date of file update>.log. Web Console begins writing data after installation and deletes the trace files after Web Console is removed.

Trace files of the application web plug-in contain the following information in addition to general data:

- KL Admin user password for unlocking the Kaspersky Industrial CyberSecurity for Nodes interface.
- Temporary password for unlocking the Kaspersky Industrial CyberSecurity for Nodes interface.
- User name and password for the SMTP mail server.
- User name and password for the proxy server.
- User name and password for the *Change application components* task.
- Account credentials and paths specified in Kaspersky Industrial CyberSecurity for Nodes tasks and policy properties.

Recording memory dumps

The memory dump file contains all information about the working memory of Kaspersky Industrial CyberSecurity for Nodes processes at the moment of application failure.

Memory dump files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed.

> Saved dump files may contain confidential data. To control access to data, you must independently ensure the security of memory dump files.

By default, memory dump files are stored in the following folder: %ProgramData%\Kaspersky Lab\KICS.5.0\Traces.

How to enable or disable memory dump recording in the Kaspersky Security Center Administration Console

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.
2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, go to the **Malfunction diagnosis** section.
4. In the **Malfunction diagnosis settings** block, click the **Settings** button.

   The **Malfunction diagnosis settings** window opens on the **Application tracing settings** tab.
5. Select the **Application dump settings** tab.
6. Use the **Create a dump file** check box to enable or disable tracing of application operation.

   By default, memory dump recording is disabled.
7. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, specify the full path to the local folder in the **Dump files folder** field.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.
8. Save your changes.

How to enable or disable memory dump recording in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and do one of the following:

   - Click the **Application properties** link in the results pane of the node.
   - Select **Application properties** in the node's context menu.

   The **Application properties** window opens.
2. Select the **Malfunction diagnosis** tab.
3. In the **Malfunction diagnosis settings** block, click the **Settings** button.

   The **Malfunction diagnosis settings** window opens.
4. Select the dump settings tab:

   - **Application dump settings**. Kaspersky Industrial CyberSecurity for Nodes records all dumps of the application.
   - **Application Console dump settings**. If Application Console and Kaspersky Industrial CyberSecurity for Nodes are installed on different computers, you can record dumps only for the Application Console.
5. Use the **Create a dump file** check box to enable or disable tracing of application operation.

   By default, memory dump recording is disabled.
6. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, click the **Browse** button and select the required folder.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.
7. Save your changes.

How to enable or disable memory dump recording in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Malfunction diagnosis** section.
5. In the **Dump file settings** block, use the **Create a dump file** check box to enable or disable tracing of application operation.

   By default, memory dump recording is disabled.
6. If necessary, change the default folder to which Kaspersky Industrial CyberSecurity for Nodes will save trace files. To do so, specify the full path to the local folder in the **Dump file folder (full path to folder, for example, C:\\Dumps\\)** field.

   > The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.
7. Save your changes.

You can also enable or disable memory dump recording in the Compact Diagnostic Interface.

Protecting dump files and trace files

Dump files and trace files contain information about the operating system, and may also contain user data. To prevent unauthorized access to such data, you can enable protection of dump files and trace files.

If protection of dump files and trace files is enabled, the files can be accessed by the following users:

- Dump files can be accessed by the system administrator and local administrator, and by the user that enabled the writing of dump files and trace files.
- Trace files can be accessed only by the system administrator and local administrator.

How to enable protection of dump files and trace files in the Kaspersky Security Center Administration Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Industrial CyberSecurity for Nodes policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **Malfunction diagnosis** section.

5. Use the **Enable dump and trace files protection** check box to enable or disable protection of dump files and trace files.

6. Save your changes.

1. In the Kaspersky Security Center Administration Console tree, select **Policies**.

2. Select the necessary policy and double-click to open the policy properties.

3. In the policy properties window, go to the **Malfunction diagnosis** section.

4. In the **Malfunction diagnosis settings** block, click the **Settings** button.

5. The **Malfunction diagnosis settings** window opens.

6. Use the **Enable dump and trace files protection** check box to enable or disable protection of dump files and trace files.

7. Save your changes.

How to enable protection of dump files and trace files in the Application Console

1. In the Application Console tree, select the **Kaspersky Industrial CyberSecurity for Nodes** node and do one of the following:

   - Click the **Application properties** link in the results pane of the node.
   - Select **Application properties** in the node's context menu.

   The **Application properties** window opens.

2. Select the **Malfunction diagnosis** tab.

3. In the **Malfunction diagnosis settings** block, click the **Settings** button.
   The **Malfunction diagnosis settings** window opens.

4. Use the **Enable dump and trace files protection** check box to enable or disable protection of dump files and trace files.

5. Save your changes.

You can also enable or disable protection of dump files and trace files in the Compact Diagnostic Interface.

Dump files and trace files that were written while protection was active remain protected even after this function is disabled.

Obtaining OS data (Kaspersky Get System Info)

After the Kaspersky Industrial CyberSecurity for Nodes application is installed, the operating system or an application may not function correctly. There is a conflict between the application and the software or drivers of the computer components.

To identify the cause of the problem, Kaspersky Technical Support requires a report from the Kaspersky Get System Info utility (hereinafter referred to as GSI). For detailed information on using the utility, refer to the Kaspersky Knowledge Base.

Sources of information about Kaspersky Industrial CyberSecurity for Nodes

You can use the following sources to find information about Kaspersky Industrial CyberSecurity for Nodes:

- Kaspersky Industrial CyberSecurity for Nodes page on the Kaspersky website
- Kaspersky Embedded Systems Security page on the Technical Support website (Knowledge Base)
- Online help
- Discussing the application on the Forum

An Internet connection is required to use online information sources.

It may not be possible to view the online help in a browser that does not support modern encryption protocols.

If you did not find a solution to your problem, contact Kaspersky Technical Support.

Kaspersky Industrial CyberSecurity for Nodes page on the Kaspersky website

On the Kaspersky Industrial CyberSecurity for Nodes page, you can review general information about the application and its functions and features.

The Kaspersky Industrial CyberSecurity for Nodes page contains a link to the online store. There you can purchase the application or renew your license.

Kaspersky Industrial CyberSecurity for Nodes page in the Knowledge Base

The Knowledge Base is a section of the Technical Support website.

On the Kaspersky Industrial CyberSecurity for Nodes page in the Knowledge Base, you can find articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Industrial CyberSecurity for Nodes but also other Kaspersky applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Industrial CyberSecurity for Nodes Help

The online help contains information about configuring and using Kaspersky Industrial CyberSecurity for Nodes.

Discussing the application on the Forum

If your question does not require an urgent answer, you can discuss it with Kaspersky experts and other users in our Forum.

In the Forum, you can view existing topics, post your own comments, and create new discussion topics.

Appendices

This section contains information that supplements the body of the document.

File extensions for quick scan

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file;

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates, xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsm for Microsoft Office Excel 2007 templates with macro support, and xlam for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

User accounts in application component rules

To configure some application components, you need to add special rules where you can select the users for whom the application will apply the rule.

Rules must be added to configure the following application components:

- Applications Launch Control
- Device Control
- Anti-Cryptor
- System Integrity Monitoring

You can add users in the following ways:

- Select from Active Directory (recommended)
- Select from the Kaspersky Security Center user list
- Add manually

Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts. For details about the security risks of using local accounts, see the Microsoft Knowledge Base. You bear full responsibility for the security of a computer if local user accounts are used; in particular this includes the responsibility for controlling and restricting access to the application settings.

The application uses the SID (Security Identifier) of the user to identify users. When using user accounts from Active Directory or from the Kaspersky Security Center user list, the application determines the SID on the Administration Server. This means the application does not place extra load on the computer to identify a user. If you added more than 1000 local user accounts to an application rule, the applications contacts the domain controller to identify the user. This means the load on the computer is increased. To optimize the performance impact on the computer, we recommend using user accounts from Active Directory or the Kaspersky Security Center user list.

Kaspersky Industrial CyberSecurity for Nodes supports embedded user and group accounts (for example, the "Everyone" group) in rules. Due to specifics of user SID detection, the application allows using embedded accounts added from Active Directory or from the Kaspersky Security Center user list only. Rules where the embedded account is added manually do not work.

Legal Information

Data provision

This section contains information about the data that the Kaspersky Industrial CyberSecurity for Nodes application may store on the device and automatically transmit to Kaspersky during its operation.

Received information is protected by Kaspersky in accordance with the law and the requirements and applicable regulations of Kaspersky. Data is transmitted over encrypted communication channels.

Data provision under the End User License Agreement

By accepting the terms of the End User License Agreement, you agree to automatically send the following data to Kaspersky:

- To support the mechanism for receiving updates – information about the installed application and licensing certificate: identifier of the application being installed and its full version, including build number, type, and license identifier, installation identifier, unique update task identifier.

- To manage confirmations for data processing – information about the status of acceptance of the License Agreement and other documents, that stipulate data transferring terms: identifier and version of License Agreement or other document, as a part of which the data processing terms are accepted or declined; an attribute, signifying the user's action (confirmation or recall of the terms acceptance); date and time of status changes of the data processing terms acceptance.

- To activate the application with an activation code - information about the type, version and localization of the installed application, versions of the installed updates, the identifier of the protected device and the identifier of the application installation on the protected device, the activation code and the unique identifier of the current license, the type, version and word size of the operating system, the name of the virtual environment when the application is installed in the virtual environment, and identifiers of the application components that are active at the time the information is provided.

The data Kaspersky receives from you when you use the application is protected and processed in accordance with the requirements established by the law and the current Kaspersky rules. Data is transmitted over encrypted communication channels. For more detailed information about processing, storage, and destruction of information obtained during the use of the application and transmitted to Kaspersky, please refer to the Privacy Policy on www.kaspersky.com/Products-and-Services-Privacy-Policy.

Local data processing

While executing the application's primary functions described in this Guide, Kaspersky Industrial CyberSecurity for Nodes locally processes and stores a sequence of data on the protected device.

The table below contains information about local processing and storing by Kaspersky Industrial CyberSecurity for Nodes of data contained in reports.

Functional area	Audit.
Type of use	Kaspersky Industrial CyberSecurity for Nodes stores the data locally and sends the data to the Administration Server. The Administration Server database stores information about application events that occur on the managed protected devices.
Storage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<product version>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Administration Server's database
Security measures	Access-control list.
Storage period	Kaspersky Industrial CyberSecurity for Nodes stores the data until the uninstallation of Kaspersky Industrial CyberSecurity for Nodes. During the Kaspersky Industrial CyberSecurity for Nodes uninstallation, all the data stored by Kaspersky Industrial CyberSecurity for Nodes on the protected device is deleted.
Purpose	Providing primary functionality.

Kaspersky Industrial CyberSecurity for Nodes does not delete events in the Windows Event Log.

Kaspersky Industrial CyberSecurity for Nodes locally processes and stores in reports the following data:

- Names and attributes of processed files and full paths to them on the scanned media.
- Actions taken on scanned files by Kaspersky Industrial CyberSecurity for Nodes.
- User actions taken on scanned files on the protected device.
- Information about accounts of users performing any actions on the protected network or protected device.
- Device Instance Path values for devices added to the Device Control rules.
- Information about processes and scripts running on the system: checksums (MD5, SHA-256) and full paths to executable files, information about digital certificates.
- Windows Firewall settings.
- Windows Event Log entries.
- Names of user accounts taking actions on scanned files on the protected device.
- Instances of executable files being started, and the types, names, checksums, and attributes of these files.
- Information about network activity: the IP addresses of blocked external devices, identifiers of compromised logon sessions from which access to protected shared resources was performed.
- Information about the Wi-Fi networks, that protected device connects to: network names and network identifiers.
- Information about the PLC projects, that are added to the protection scope, including PLC connection settings (IP, rack and slot numbers, password) and firmware checksums.
- Information about the Windows USN Journal status.

The table below contains information about local processing and storing by Kaspersky Industrial CyberSecurity for Nodes of data about parameters specified by a user.

Kaspersky Industrial CyberSecurity for Nodes processes and stores only the parameters' data specified by a user.

Processing and storing of data about parameters specified by a user

Functional area	Auto-remediation, Sandbox integration.
Type of use	Kaspersky Industrial CyberSecurity for Nodes stores the data about parameters locally and sends the data to the Administration Server. The Administration Server's database stores information about parameters of the managed protected devices.
Storage	%ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<product version>\
Security measures	Access-control list.
Storage period	Kaspersky Industrial CyberSecurity for Nodes stores the data until the uninstallation of Kaspersky Industrial CyberSecurity for Nodes. During the Kaspersky Industrial CyberSecurity for Nodes uninstallation, all the data stored by Kaspersky Industrial CyberSecurity for Nodes on the protected device is deleted.
Purpose	Providing primary functionality.

Kaspersky Industrial CyberSecurity for Nodes does not delete the data about parameters exported into configuration file.

Kaspersky Industrial CyberSecurity for Nodes does not delete Quarantine objects and Backup objects if the **Export quarantine objects** and **Export Backup objects** check boxes are selected in the Setup Wizard.

Kaspersky Industrial CyberSecurity for Nodes locally processes and stores the following data about parameters specified by a user:

- Information about objects placed in Quarantine or Backup.
- Information about the settings configured via the Application Console or via the Administration Plug-in, for example:
  - Kaspersky Industrial CyberSecurity for Nodes password, names of user accounts under which Kaspersky Industrial CyberSecurity for Nodes tasks are run.
  - The name of user account used for proxy server authentication.
  - The addresses of network folders or folders on the HTTP or FTP servers used as user-defined update sources.
  - Information about the Wi-Fi networks.
  - Information about the PLC projects, that are added to the protection scope, including PLC connection settings and firmware checksums.
  - IP addresses and identifiers of blocked logon sessions.
  - Windows Firewall settings.

- Checksums (MD5, SHA-256) and paths to executable files added to the Application Launch Control task rules.
- Device Instance Path values for devices added to the Device Control rules.
- Information about folders included in scopes of Kaspersky Industrial CyberSecurity for Nodes tasks.
- Information about events in the Windows Event Log.
- Information about files detected through the use of iSwift or iCheker technology.
- Checksums (MD5, SHA-256) and paths to the files added to the Trusted Zone.
- Information about added license keys.
- Information about digital certificates.
- Checksums of the files, digital certificates data, full paths to the files (SDC database, files for Baseline File Integrity Monitor task).
- Temporary files created when the application scans the archives.
- Information in %SystemRoot%.

- Data about files processed by the Kaspersky Industrial CyberSecurity for Nodes, for example, checksums (MD5, SHA-256) of files, information about digital certificates, full paths to files.

Kaspersky Industrial CyberSecurity for Nodes processes and stores data as part of the application's basic functionality, including to log application events and receive diagnostic data. Locally processed data is processed and protected in accordance with the configured and applied application settings.

Kaspersky Industrial CyberSecurity for Nodes lets you configure the level of protection for data processed locally: you can change user privileges to access process data, change data retention periods for such data, entirely or partially disable functionality that involves data logging, and change the path and attributes of the folder on the drive where data is logged.

Detailed information about configuring application functionality that involves data processing can be found in the corresponding sections of this Guide.

Local data processing by means of the application auxiliary components

The Kaspersky Industrial CyberSecurity for Nodes installation package comprises the application auxiliary components, which can be installed on your device even if Kaspersky Industrial CyberSecurity for Nodes is not installed on it.

While performing the main functions of the application described in this Guide, the application auxiliary components locally process and store a set of data on the protected device where they are installed, even if they are installed separately from Kaspersky Industrial CyberSecurity for Nodes.

The table below contains information about local processing and storing by Kaspersky Industrial CyberSecurity for Nodes of data written in dump and trace files.

By default, Kaspersky Industrial CyberSecurity for Nodes does not write dump and trace files.

Processing and storing of data written in dump and trace files

Storage	By default the folder to which dump and trace files are saved is not specified. You can specify the folder
Security measures	Kaspersky Industrial CyberSecurity for Nodes does not restrict access to dump and trace files.
Storage period	Kaspersky Industrial CyberSecurity for Nodes does not delete dump and trace files.
Purpose	Providing technical support.

Kaspersky Industrial CyberSecurity for Nodes locally processes and stores the following data written in dump and trace files:

- Information about actions performed by Kaspersky Industrial CyberSecurity for Nodes on the protected device.
- Information about objects processed by Kaspersky Industrial CyberSecurity for Nodes.
- Information about errors that occurred during the running of Kaspersky Industrial CyberSecurity for Nodes.

The data processed by the auxiliary components is not automatically sent to Kaspersky or other third-party systems.

By default, all data locally processed by the application auxiliary components during the operation is deleted after removal of these components.

The exception is trace files of auxiliary application components. We recommend that you delete these files manually.

You can find the detailed information about working with files containing diagnostic data of the application auxiliary components in the corresponding sections of this Guide.

Data provision when using Detection and Response solutions

Computers with installed Kaspersky Industrial CyberSecurity for Nodes accumulate data prepared for automatic transmission to servers of Detection and Response solutions. Files are stored on computers in plain, non-encrypted form.

The specific set of data depends on the solution within which Kaspersky Industrial CyberSecurity Endpoint Detection and Response is used.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response

All data that the application stores locally on the computer, is deleted from the computer when Kaspersky Industrial CyberSecurity for Nodes is uninstalled.

Data received as a result of IOC Scan task execution (standard task)

Kaspersky Industrial CyberSecurity for Nodes automatically submits data on the *IOC Scan* task execution results to Kaspersky Security Center.

The data in the *IOC Scan* task execution results may contain the following information:

- IP address from the ARP table
- Physical address from the ARP table
- DNS record type and name
- IP address of the protected computer
- Physical address (MAC-address) of the protected computer
- Identifier in the event log entry
- Data source name in the log
- Log name
- Event time
- MD5 and SHA256 hashes of the file
- Full name of the file (including path)
- File size
- Remote IP address and port to which connection was established during scan
- Local adapter IP address
- Port open on the local adapter
- Protocol as a number (in accordance with the IANA standard)
- Process name
- Process arguments
- Path to the process file
- Windows identifier (PID) of the process
- Windows identifier (PID) of the parent process
- User account that started the process
- Date and time when the process was started

- Service name
- Service description
- Path and name of the DLL service (for svchost)
- Path and name of the service executable file
- Windows identifier (PID) of the service
- Service type (for example, a kernel driver or adapter)
- Service status
- Service launch mode
- User account name.
- Volume name
- Volume letter
- Volume type
- Windows registry value
- Registry hive value
- Registry key path (without hive and value name)
- Registry setting
- System (environment)
- Name and version of the operating system that is installed on the computer
- Network name of the protected computer
- Domain or group the protected computer belongs to
- Browser name
- Browser version
- Time when the web resource was last accessed
- URL from the HTTP request
- Name of the account used for the HTTP request
- File name of the process that made the HTTP request
- Full path to the file of the process that made the HTTP request
- Windows identifier (PID) of the process that made the HTTP request

- HTTP referer (HTTP request source URL)
- URI of the resource requested over HTTP
- Information about the HTTP user agent (the application that made the HTTP request)
- HTTP request execution time
- Unique identifier of the process that made the HTTP query

Data for creating a threat development chain

Data for creating a threat development chain is stored for seven days by default. The data is automatically sent to Kaspersky Security Center.

Data for creating a threat development chain may contain the following information:

- Incident date and time
- Detection name
- Scan mode
- Status of the last action related to the detection
- Reason why the detection processing failed
- Detected object type
- Detected object name
- Threat status after the object is processed
- Reason why execution of actions on the object failed
- Actions performed to roll back malicious actions
- Information about the processed object:
  - Unique identifier of the process
  - Unique identifier of the parent process
  - Unique identifier of the process file
  - Windows process identifier (PID)
  - Process command line
  - User account that started the process
  - Code of the logon session in which the process is running

- Type of the session in which the process is running
- Integrity level of the process being processed
- Membership of the user account that started the process in the privileged local and domain groups
- Identifier of the processed object
- Full name of the processed object
- Identifier of the protected device
- Full name of the object (local file name or downloaded file web address)
- MD5 or SHA256 hash of the processed object
- Type of the processed object
- Creation date of the processed object
- Date when the processed object was last modified
- Size of the processed object
- Attributes of the processed object
- Organization that signed the processed object
- Result of the processed object digital certificate verification
- Security identifier (SID) of the processed object
- Time zone identifier of the processed object
- Web address of the processed object download (only for files on disk)
- Name of the application that downloaded the file
- MD5 and SHA256 hashes of the application that downloaded the file
- Name of the application that last modified the file
- MD5 and SHA256 hashes of the application that last modified the file
- Number of processed object starts
- Date and time when the processed object was first started
- Unique identifiers of the file
- Full name of the file (local file name or downloaded file web address)
- Path to the processed Windows registry variable
- Name of the processed Windows registry variable

- Value of the processed Windows registry variable
- Type of the processed Windows registry variable
- Indicator of the processed registry key membership in the autorun point
- Web address of the processed web request
- Link source of the processed web request
- User agent of the processed web request
- Type of the processed web request (`GET` or `POST`)
- Local IP port of the processed web request
- Remote IP port of the processed web request
- Connection direction (inbound or outbound) of the processed web request
- Identifier of the process into which the malicious code was embedded

Kaspersky Endpoint Detection and Response Expert (on-premises)

All data that the application stores locally on the computer, is deleted from the computer when Kaspersky Industrial CyberSecurity for Nodes is uninstalled.

Service data

The Kaspersky Industrial CyberSecurity for Nodes built-in agent stores the following data locally:

- Data required for integration with the EDR Expert (on-premises) component:
  - Address and port for connecting to the KATA Central Node server
  - Address and port for connecting to the telemetry transmission server
  - Address and port for connecting to the response server
  - Information about certificates used for integration with KATA Central Node
  - Information about certificates used for integration with the telemetry transmission server
  - Information about certificates used for integration with the response server
- Quarantined files

Data from transmitted telemetry events

- **Telemetry data**
  - Data on files:
    - Unique identifiers of the file
    - File type
    - Full file path
    - File size
    - File attributes
    - Zone identifier
    - Date and time when the file was created
    - Date and time when the file was last modified
    - Original file name
    - Application name
    - Application version
    - Application vendor
    - File description
    - File version
    - MD5 and SHA256 hashes of the object
    - Result of file signature verification
    - Certificate issuer name
    - Certificate holder name
    - Certificate serial number
  - Data about AMSI scan:
    - Unique identifier of the process that initiated the activity
    - Content type of the object passed to AMSI
    - Content of the object passed to AMSI

    - Object name
    - MD5 and SHA256 hashes of the object
- Data about application blocking:
    - Unique identifier of the process that initiated the application blocking
    - Unique identifier of the parent process
    - Unique system identifier of the process
    - Command used to start a process
    - Login session ID
    - Process integrity level
    - Process status
    - Unique identifier of the process file
    - Process command line
    - List of unique identifiers of interpreted files
- Data about blocked file openings:
    - Unique identifier of the process that initiated the file opening
    - Unique identifiers of the file
- Data about driver loading:
    - Unique identifier of the loaded driver
- Data about events:
    - Unique identifier of the event
    - Event date and time
- Data about file modification:
    - Unique identifier of the process that initiated the file modification
    - Unique identifiers of the file
    - Type of the modification operation
    - Flag indicating that the file will be deleted after the computer is restarted
    - Unique identifier of the modified file
    - Unique identifier of the file before modification

    - Set of bit flags that determine how the file was opened
    - Data about operations on the access control list
    - Data about changes to the ownership or parent group of the file
- Data about login session:
    - Login session ID
    - User name of the user who logged in
    - User account type
    - Session type
- Data about network connections:
    - Unique identifier of the process that initiated the connection
    - Local IP address used to initiate the connection
    - Remote IP address of the connection endpoint
    - Connection direction
    - Data transfer protocol
    - HTTP method
    - Path without the host name
    - Host name
    - Dynamic process state at the moment of the connection
    - Flag indicating that the connection is open at the raw socket level
    - TLS version used in the connection session
    - Name of the TLS server
    - MD5 and SHA1 hashes of the TLS server certificate
    - List of Subject Alternative Names (SAN) of the certificate
    - TLS certificate issuer name
    - Certificate serial number
    - Encryption algorithm used
    - Start and end dates of the certificate

    - JA3 fingerprint of the TLS client
    - JA3S fingerprint of the server
- Data captured while listening on a network port:
    - Unique identifier of the process that initiated the connection
- Command line input data:
    - Unique identifier of the process that initiated the console input
    - Console input type
    - Text entered by a user or a process
- Data about process creation:
    - Unique identifier of the process
    - Unique identifier of the parent process
    - Unique system identifier of the process
    - Command used to start a process
    - Login session ID
    - Process integrity level
    - Unique identifier of the process file
    - List of unique identifiers of interpreted files
    - Process type
- Data about the module loaded by the process:
    - Unique identifier of the process that initiated the download
    - Full path to the file that was uploaded to the process
    - Unique identifier of the module file
    - Full qualified name of the .NET assembly, if the loaded file is a .NET module
    - Flags of the .NET assembly defined in its manifest
- Data about process termination:
    - Unique identifier of the terminated process

- Data about registry modification:
  - Unique identifier of the process that initiated the registry modification
  - Type of registry operation
  - Full path to the registry key
  - Name of the value within a registry key
  - Type of data stored in the registry key value
  - Data specified in the registry key value
  - Name of the key before renaming
  - Information regarding a change in ownership of the key or primary key group
  - List of changes to the access control list (ACL) of the key
- Data about the detected threat and its processing:
  - Flag indicating that threat detection ran in background
  - Threat verdict
  - Verdict name
  - Unique identifier of the database record
  - Time when the threat record was saved in the database
  - Threat processing mode
  - Infected object type
  - Infected object name
  - MD5 and SHA256 hashes of the object
  - Unique identifier of infected object
  - Unique identifier of the process that downloaded the infected object from the internet
  - URL from which the infected object was downloaded
  - Sender email address that sent the infected object
  - Network protocol through which the infected object was received
  - Local address from which the infected object was received
  - External address from which the infected object was received

    - Object content type
    - Object content
- Data about access to processes:
    - Unique identifier of the process that attempted access
    - Unique identifier of the target process that was accessed
    - Set of rights requested from the target process
    - Operation type
    - Set of calls at the moment of accessing a process
    - Source process descriptor
    - Target process descriptor
- Data about DNS:
    - Unique identifier of the process that initiated the DNS query
    - DNS server IP address
    - Flags that manage the behavior of a DNS query
    - Request completion status
    - Fully qualified domain name specified in the DNS query
    - Data type in the DNS query
    - DNS server responses
- Data about code injection:
    - Unique identifier of the process that attempted to inject code
    - Used access method
    - Set of calls at the time the injected code was detected
    - Unique identifier of the target process to which the code was uploaded
    - Data about changes in the command sequence of the target process
    - Target process address
    - Name of the DLL library that was uploaded to the target process
    - Full path to the DDL file

- Data about operations with named channels:
  - Unique identifier of the process that created or connected to the channel
  - Full name of the named channel
  - Operation type (creation or connection)
- Data about WMI queries:
  - Unique identifier of the process that initiated the WMI operation
  - WMI operation type
  - Name of the target device for the WMI query
  - User account that initiated the WMI query
  - Text of the WMI query
  - Namespace in which the WMI query is performed
  - WMI filter name
  - Name of the consumer object
  - Text describing the action of the consumer object
- Data about LDAP queries:
  - Unique identifier of the process that made the LDAP query
  - Search scope of LDAP queries
  - LDAP filter
  - Parameter that specifies the Active Directory partition to which the query was directed
  - LDAP search attributes
- Data about connected USB devices:
  - USB device operation type
  - USB device type
  - Identifier of the USB device
  - USB device name
  - Path to the USB device
  - Flag indicating that the USB device is a system drive
- Data about creation, deletion, and modification of a scheduled task

- Data about creation, deletion, and modification of services
- Data about mounting/unmounting of the file system
- Data about the operation of the EDR Expert on-premise component:
  - Information about starting/stopping the agent
  - Information about installing/uninstalling the agent
  - Unique identifier for the agent start
  - System identifier of the agent process
  - Unique identifier of the agent process
  - Reason for the termination of the agent
  - Agent process termination code
- Event filtering settings:
  - Module names
  - Full paths to objects
  - MD5 and SHA256 hashes of the objects
  - Identifiers of the entries in Windows event log
  - Digital certificate settings
  - Traffic direction, IP addresses, ports, protocols, full paths to executable files
  - User names
  - User logon types
  - Types of telemetry events for which filters are applied

Data from requests of the EDR Expert component to the built-in agent of Kaspersky Industrial CyberSecurity for Nodes

- General task settings:
  - Task type
  - Task schedule settings
  - Names and passwords of the accounts under which the tasks can be run
  - Versions of settings

- Identifiers of quarantined objects
- Paths to the objects
- MD5 and SHA256 hashes of the objects
- Command line to start the process with the arguments
- Flags of the additional actions performed upon completion of tasks
- IOC file identifiers to be retrieved from the server
- IOC files
- Service name
- Service startup type
- Folders for which the results of the *Get forensic* task must be received
- Masks of the object names and extensions for the *Get forensic* task

- Network isolation settings:
  - Types of settings
  - Versions of settings
  - Lists of network isolation exclusions and exclusion settings: traffic direction, IP addresses, ports, protocols, and full paths to executable files
  - Flags of the additional actions
  - Time of automatic isolation disabling
- Execution prevention settings:
  - Types of settings
  - Versions of settings
  - Lists of execution prevention rules and rule settings: paths to objects, types of objects, MD5 and SHA256 hashes of objects
  - Flags of the additional actions

Data from queries from Kaspersky Industrial CyberSecurity for Nodes to the EDR Expert component

When integrating with the EDR Expert (on-premises) solution, the following data is stored locally on the computers.

- In synchronization requests:
  - Unique ID
  - Basic part of the server web address
  - Computer name
  - Computer IP address
  - Computer MAC address
  - Local time on the computer
  - Kaspersky Industrial CyberSecurity for Nodes self-defense status
  - Name and version of the operating system that is installed on the computer
  - Kaspersky Industrial CyberSecurity for Nodes version
  - Versions of the application settings and task settings
  - Task statuses: identifiers of tasks, execution statuses, error codes
- In requests for obtaining files from the server:
  - Unique identifiers of files
  - Unique identifier of Kaspersky Industrial CyberSecurity for Nodes
  - Unique identifiers of certificates
  - Basic part of the web address of the server with the Central Node component installed
  - Host IP address
- In the reports on task execution results:
  - Host IP address
  - Information about the objects detected during an IOC scan or YARA scan
  - Flags of the additional actions performed upon completion of tasks
  - Task execution errors and return codes
  - Task completion statuses

    - Task completion time
    - Versions of the settings used for execution of the tasks
    - Information about the objects submitted to the server, quarantined objects, and objects restored from quarantine: paths to objects, MD5 and SHA256 hashes, identifiers of quarantined objects
    - Information about the processes started or stopped on a computer at the server's request: PID and UniquePID, error code, MD5 and SHA256 hashes of the objects
    - Information about the services started or stopped on a computer at the server's request: service name, startup type, error code, MD5 and SHA256 hashes of file images of the services
    - Information about the objects for which a memory dump was made for a YARA scan (paths, dump file identifier)
    - Files requested by the server
- Data on running processes:
    - Executable file name, including full path and extension
    - Process autorun parameters
    - Process ID
    - Login session ID
    - Login session name
    - Date and time when the process was started
    - MD5 and SHA256 hashes of the object
- Data on files:
    - File path
    - File name
    - File size
    - File attributes
    - Date and time when the file was created
    - Date and time when the file was last modified
    - File description
    - Company name
    - MD5 and SHA256 hashes of the object
    - Registry key (for autorun points)

- Data in errors that occur when information about objects was retrieved:
  - Full name of the object that was processed when an error occurred
  - Error code
- Data in YARA scan results:

  The built-in agent of Kaspersky Industrial CyberSecurity for Nodes automatically transfers YARA scan results to Kaspersky Anti Targeted Attack Platform to build a threat development chain.

  The data is temporarily stored locally in the queue for sending task execution results to the Kaspersky Anti Targeted Attack Platform server. The data is deleted from the temporary storage once it has been sent.

  - MD5 and SHA256 hashes of the file
  - Full name of the file
  - File path
  - File size
  - Process name
  - Process arguments
  - Path to the process file
  - Windows identifier (PID) of the process
  - Windows identifier (PID) of the parent process
  - User account that started the process
  - Date and time when the process was started
- Data in IOC scan results:
  - IP address from the ARP table
  - Physical address from the ARP table
  - DNS record name
  - DNS record type
  - Host name
  - IP address
  - Event ID in the log
  - Data source name in the log
  - Log name
  - User name

- Date and time the event was generated, in the ISO format
- MD5 and SHA256 hashes of the file
- Full name of the file
- File size
- Remote IP address and port to which connection was established during scan
- IP address and port of the local adapter
- Protocol
- Process name
- Process arguments
- Path to the process file
- Windows identifier (PID) of the process
- Windows identifier (PID) of the parent process
- User account that started the process
- Date and time when the process was started
- Path to the registry key
- Registry key name
- Text value of the registry key
- Service name
- Service description
- Path and name of the DLL service
- Path and name of the service executable file
- Windows identifier (PID) of the service
- Service type
- Service status
- Service launch mode
- Operating system name
- Operating system version
- Computer network name without domain

- Domain or workgroup
- User name
- Volume name
- Volume letter
- Volume type

Kaspersky Industrial CyberSecurity for Networks Integration

All data that the application stores locally on the computer, is deleted from the computer when Kaspersky Industrial CyberSecurity for Nodes is uninstalled.

Service data

The Kaspersky Industrial CyberSecurity for Nodes built-in agent stores the following data locally:

- Data required for integration with Kaspersky Industrial CyberSecurity for Networks:
  - The address and port for connecting to the Kaspersky Industrial CyberSecurity for Networks server
  - Information about certificates for integration with Kaspersky Industrial CyberSecurity for Networks
- Quarantined files

Data from transmitted telemetry events

- **Data about files**
  - Unique identifiers of the file
  - File type
  - Full file path
  - File size
  - File attributes
  - ZoneId
  - Date and time when the file was created
  - Date and time when the file was last modified

- The date and time the file attributes were modified
- Original file name
- Application name
- Application version
- Application vendor
- File description
- File version
- MD5 and SHA256 hashes of the object
- Result of file signature verification
- Date and time when the file signature was created
- Certificate chains used in the signature file:
  - Certificate chain type
  - Information about certificates in the chain:
    - Certificate issuer name
    - Certificate holder name
    - Certificate serial number
    - Certificate thumbprint algorithm
    - Certificate thumbprint
    - Certificate validity period

- **Data about HTTP queries**
  - Unique identifier of the process that sent the query
  - Local IP address and port
  - Remote IP address and port
  - Data transfer protocol
  - Connection direction
  - Information about the HTTP request:
    - HTTP method
    - Path without a domain name

        - Host name
        - List of HTTP headers:
            - Name
            - Value
- **Alert Details**
    - Detection ID
    - Detection date and time
    - Detection name
    - Encryption mode
    - Status of the last action related to the detection
    - Reason why the detection processing failed
    - Object type
    - Object name
    - MD5 and SHA256 hashes of the object
    - Actions to eliminate the threat
    - Information about the reputation of the object in the Kaspersky Security Network:
        - Group in which the application is placed
        - Number of Kaspersky Security Network users who use the application
        - Countries where the application is most widely used
        - Date and time of the first appearance of the application in the Kaspersky Security Network
        - Date and time the information was received from Kaspersky Security Network
- **Login session data**
    - Session ID
    - The name of the user account used to log in
    - User account type
    - Session type
    - IP address of the device from which the login attempt was made
    - IP address of the device for which the login attempt was made

- Information about this session having elevated and administrator privileges
- Information about associated login sessions
- Application protocol for a remote session
- Remote access session protocol.

- **Data about session termination**
  - Session ID
  - The name of the user account used to log in
  - User account type
  - Session type
  - IP address of the device from which the login attempt was made
  - IP address of the device for which the login attempt was made
  - Information about this session having elevated and administrator privileges
  - Information about associated login sessions
  - Application protocol for a remote session
  - Remote access session protocol.
  - Session ID
- **Data about network communication**
  - Start and end of the time interval over which the data was collected
  - List of connections:
    - Local IP address of the computer
    - Local MAC address of the computer
    - Remote IP address of the computer
    - Remote MAC address of the computer
    - Gateway IP address
    - Number of transmitted data packets
    - Number of received data packets.
    - Total number of bytes transferred
    - Data transfer protocol

        - EtherType
        - Payload prefix of the first packet in the interval
        - IPv4 address of the network interface through which the communication was captured
- **Data about network connection**
    - Unique identifier of the process that initiated the connection
    - Data transfer protocol
    - Local IP address used to initiate the connection
    - Remote IP address of the connection endpoint
    - Information about the HTTP request:
        - HTTP method
        - Path without a domain name
        - Host name
        - List of HTTP headers:
            - Name
            - Value
    - Dynamic process state at the moment of the connection
    - Connection direction
    - Dynamic process state
    - EtherType
- **Data captured while listening on a network port**
    - Unique identifier of the process that initiated the connection
    - Data transfer protocol
    - Local address
    - Dynamic process state at the moment of the connection
- **Result of connection verification**
    - Host network settings:
        - Network interface description
        - DNS domain name

        - Local MAC address of the computer
        - IP connection metric number
        - List of IP addresses:
            - IP address
            - Network mask
            - Gateway IP address
            - Gateway MAC address
    - List of installed patches:
        - Patch number
        - Patch installation date
    - Device model
    - Device vendor
    - Host ID in Kaspersky Security Center
    - Description of installed Kaspersky antivirus:
        - Component name of installed Kaspersky antivirus
        - Component version of installed Kaspersky antivirus
        - Database version of installed Kaspersky antivirus component
        - Date of last database update of installed Kaspersky antivirus component
        - Component status of installed Kaspersky antivirus
        - List of license keys:
            - Key serial number
            - Key type
            - Key expiration date
            - Key status
- **Data about process creation**
    - Unique identifier of the process
    - Unique identifier of the parent process
    - Unique system identifier of the process

- Command used to start a process
- Login session ID
- Terminal session ID
- Unique identifier of the process file
- Process integrity level
- List of token permissions:
  - Rights
  - Attributes of rights
- List of unique identifiers of interpreted files
- Process status
- Command used to start a process

- **Data about process termination**
  - Unique identifier of infected object
- **Data about detected threat**
  - Threat information:
    - Threat verdict
    - AMR record number
    - Antivirus database version
    - Threat detection mode
    - Threat UUID
    - Protection technology
    - Unique identifier of the threat
    - Protection technology
  - Information about infected object:
    - Infected object type
    - Infected object name
    - MD5 and SHA256 hashes of the object
    - Unique identifier of infected process

        - Unique identifier of infected object
        - Unique identifier of the process that downloaded the infected object from the internet
        - URL from which the infected object was downloaded
        - Sender email address that sent the infected object
        - Network protocol type (according to IANA)
        - Local network address
        - External network address from which the infected object was received
        - Object content type
        - Context of detected threat
        - Object content
    - Flag indicating that threat detection ran in background
    - Local physical address
    - Physical address from which the infected object was received
- **Data about threat processing**
    - Threat information:
        - Threat verdict
        - AMR record number
        - Antivirus database version
        - Threat detection mode
        - Threat UUID
        - Protection technology
    - Information about infected object:
        - Infected object type
        - Infected object name
        - MD5 and SHA256 hashes of the object
        - Unique identifier of infected process
        - Unique identifier of infected object
        - Network protocol type (according to IANA)

        - External network address from which the infected object was received
        - Local network address
    - Threat processing status
    - Reason why the threat could not be remediated
    - Local physical address
- **Data about users**
    - User SID
    - User ID
    - User name
    - Full name of the user
    - User description
    - Whether the account is enabled or disabled
    - Whether the account is blocked
    - Whether the password has expired
    - Whether a password change is required
    - Whether the user can change the password
    - User account type
    - Whether automatic login is enabled for this account
    - List of groups the user belongs to
    - Date of last password change.
    - Date of the last session termination.

Data from Kaspersky Industrial CyberSecurity for Networks requests to the built-in agent of Kaspersky Industrial CyberSecurity for Nodes

- General task settings:
    - Task type
    - Task schedule settings
    - Names and passwords of the accounts under which the tasks can be run

- Versions of settings
- Identifiers of quarantined objects
- Paths to the objects
- MD5 and SHA256 hashes of the objects
- Command line to start the process with the arguments
- Flags of the additional actions performed upon completion of tasks
- Service name
- Service startup type

- Network isolation settings:
  - Types of settings
  - Versions of settings
  - Lists of network isolation exclusions and exclusion settings: traffic direction, IP addresses, ports, protocols, and full paths to executable files
  - Flags of the additional actions
  - Time of automatic isolation disabling
- Execution prevention settings:
  - Types of settings
  - Versions of settings
  - Lists of execution prevention rules and rule settings: paths to objects, types of objects, MD5 and SHA256 hashes of objects
  - Flags of the additional actions

Data from Kaspersky Industrial CyberSecurity for Nodes requests to Kaspersky Industrial CyberSecurity for Networks

When integrated with Kaspersky Industrial CyberSecurity for Networks, the following data is stored locally on computers.

- In synchronization requests:
  - Unique ID
  - Basic part of the server web address
  - Computer name

- Computer IP address
- Computer MAC address
- Local time on the computer
- Kaspersky Industrial CyberSecurity for Nodes self-defense status
- Name and version of the operating system that is installed on the computer
- Kaspersky Industrial CyberSecurity for Nodes version
- Versions of the application settings and task settings
- Task statuses: identifiers of tasks, execution statuses, error codes

- In requests for obtaining files from the server:
  - Unique identifiers of files
  - Unique identifier of Kaspersky Industrial CyberSecurity for Nodes
  - Unique identifiers of certificates
  - Basic part of the web address of the server with the Central Node component installed
  - Host IP address
- In the reports on task execution results:
  - Host IP address
  - Flags of the additional actions performed upon completion of tasks
  - Task execution errors and return codes
  - Task completion statuses
  - Task completion time
  - Versions of the settings used for execution of the tasks
  - Information about the objects submitted to the server, quarantined objects, and objects restored from quarantine: paths to objects, MD5 and SHA256 hashes, identifiers of quarantined objects
  - Information about the processes started or stopped on a computer at the server's request: PID and UniquePID, error code, MD5 and SHA256 hashes of the objects
  - Information about the services started or stopped on a computer at the server's request: service name, startup type, error code, MD5 and SHA256 hashes of file images of the services
  - Files requested by the server

- Data on running processes:
  - Executable file name, including full path and extension
  - Process autorun parameters
  - Process ID
  - Login session ID
  - Login session name
  - Date and time when the process was started
  - MD5 and SHA256 hashes of the object
- Data on files:
  - File path
  - File name
  - File size
  - File attributes
  - Date and time when the file was created
  - Date and time when the file was last modified
  - File description
  - Company name
  - MD5 and SHA256 hashes of the object
  - Registry key (for autorun points)
- Data in errors that occur when information about objects was retrieved:
  - Full name of the object that was processed when an error occurred
  - Error code

SIEM Integration

All data that the application stores locally on the computer, is deleted from the computer when Kaspersky Industrial CyberSecurity for Nodes is uninstalled.

When integrated with SIEM systems, information about connection settings as well as all events in Windows logs are transmitted.

The main Windows Event Logs are System, Security, Application, ForwardedEvents, and HardwareEvents. Users can also create and work with custom logs to meet their specific requirements.

Data provision when using Kaspersky Security Network

The set of data that Kaspersky Industrial CyberSecurity for Nodes sends to Kaspersky depends on the type of license and the Kaspersky Security Network usage settings.

Use of KSN under license on no more than 4 computers

By accepting the Kaspersky Security Network Statement, you agree to automatically transmit the following information:

- information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update;
- information about files and URL addresses to be scanned: checksums of the scanned file (MD5, SHA2-256, SHA1) and file patterns (MD5), the size of the pattern, type of the detected threat and its name according to Rightholder's classification, identifier for the anti-virus databases, URL address for which the reputation is being requested, as well as the referrer URL address, the connection's protocol identifier and the number of the port being used;
- ID of the scan task that detected the threat;
- information about digital certificates being used needed to verify their authenticity: the checksums (SHA256) of the certificate used to sign the scanned object and the certificate's public key;
- identifier of the Software component performing the scan;
- IDs of the anti-virus databases and of the records in these anti-virus databases;
- Information about activation of the Software on the Computer: signed header of the ticket from the activation service (identifier of the regional activation center, checksum of the activation code, checksum of the ticket, ticket creation date, unique identifier of the ticket, ticket version, license status, start/end date and time of ticket validity, unique identifier of the license, license version), identifier of the certificate used to sign the ticket header, checksum (MD5) of the key file;
- Information about the Rightholder's Software: full version, type, version of the protocol used to connect to Kaspersky services.

Use of KSN under license on 5 or more computers

By accepting the Kaspersky Security Network Statement, you agree to automatically transmit the following information:

If the **Kaspersky Security Network** check box is selected and the **Enable extended KSN mode** check box is cleared, the application sends the following information:

- information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update;
- information about files and URL addresses to be scanned: checksums of the scanned file (MD5, SHA2-256, SHA1) and file patterns (MD5), the size of the pattern, type of the detected threat and its name according to Rightholder's classification, identifier for the anti-virus databases, URL address for which the reputation is being requested, as well as the referrer URL address, the connection's protocol identifier and the number of the port being used;
- ID of the scan task that detected the threat;
- information about digital certificates being used needed to verify their authenticity: the checksums (SHA256) of the certificate used to sign the scanned object and the certificate's public key;
- identifier of the Software component performing the scan;
- IDs of the anti-virus databases and of the records in these anti-virus databases;
- Information about activation of the Software on the Computer: signed header of the ticket from the activation service (identifier of the regional activation center, checksum of the activation code, checksum of the ticket, ticket creation date, unique identifier of the ticket, ticket version, license status, start/end date and time of ticket validity, unique identifier of the license, license version), identifier of the certificate used to sign the ticket header, checksum (MD5) of the key file;
- Information about the Rightholder's Software: full version, type, version of the protocol used to connect to Kaspersky services.

If the **Enable extended KSN mode** check box is selected in addition to the **Kaspersky Security Network** check box, the application sends the following information in addition to the information listed above:

- information about the results of categorization of the requested web-resources, which contains the processed URL and IP address of the host, the version of the Software's component that performed the categorization, the method of categorization and set of the categories defined for the web-resource;
- information about the software installed on the Computer: names of the software applications and software vendors, registry keys and their values, information about files of the installed software components (checksums (MD5, SHA2-256, SHA1), name, path to the file on the Computer, size, version and the digital signature);
- information about the state of anti-virus protection of the Computer: the versions and the release timestamps of the anti-virus databases being used, the ID of the task and the ID of Software that performs scanning;
- information about files being downloaded by the End User: the URL and IP addresses of the download and the download pages, download protocol identifier and connection port number, the status of the URLs as malicious or not, file's attributes, size and checksums (MD5, SHA2-256, SHA1), information about the process that downloaded the file (checksums (MD5, SHA2-256, SHA1), creation/build date and time, autoplay status, attributes, names of packers, information about signatures, executable file flag, format identifier, and entropy), file name and its path on the Computer, the file's digital signature and timestamp of its generation, the URL address where detection occurred, the script's number on the page that appears to be suspicious or harmful, information about HTTP requests generated and the response to them;

- information about the running applications and their modules: data about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the sign of trusted program or process, the full path to the process's files and their checksums (MD5, SHA2-256, SHA1), and the starting command line, level of the process's integrity, a description of the product that the process belongs to (the name of the product and information about the publisher), as well as digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes (their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them on the Computer), PE-file header information, names of packers (if the file was packed);

- information about all potentially malicious objects and activities: name of the detected object and full path to the object on the computer, checksums of processed files (MD5, SHA2-256, SHA1), detection date and time, names and sizes of infected files and paths to them, path template code, executable file flag, indicator of whether the object is a container, names of the packer (if the file was packed), file type code, file format ID, list of actions performed by malware and the decision made by the software and user in response to them, IDs of the anti-virus databases and of the records in these anti-virus databases that were used to make the decision, indicator of a potentially malicious object, the name of the detected threat according to the Rightholder's classification, the level of danger, the detection status and detection method, reason for inclusion into the analyzed context and sequence number of the file in the context, checksums (MD5, SHA2-256, SHA1), the name and attributes of the executable file of the application through which the infected message or link was transmitted, depersonalized IP addresses (IPv4 and IPv6) of the host of the blocked object, file entropy, file autorun indicator, time when the file was first detected in the system, the number of times the file has been run since the last statistics were sent, information about the name, checksums (MD5, SHA2-256, SHA1) and size of the mail client through which the malicious object was received, ID of the software task that performed the scan, indicator of whether the file reputation or signature was checked, file processing result, checksum (MD5) of the pattern collected for the object, the size of the pattern in bytes, and the technical specifications of the applied detection technologies;

- information about scanned objects: the assigned trust group to which and/or from which the file has been placed, the reason the file was placed in that category, category identifier, information about the source of the categories and the version of the category database, the file's trusted certificate flag, name of the file's vendor, file version, name and version of the software application which includes the file;

- information about vulnerabilities detected: the vulnerability ID in the database of vulnerabilities, the vulnerability danger class;

- information about emulation of the executable file: file size and its checksums (MD5, SHA2-256, SHA1), the version of the emulation component, emulation depth, an array of properties of logical blocks and functions within logical blocks obtained during the emulation, data from the executable file's PE headers;

- the IP addresses of the attacking computer (IPv4 and IPv6), the number of the port on the Computer that the network attack is directed at, identifier of the protocol of the IP packet containing the attack, the attack's target (organization name, website), flag for the reaction to the attack, the attack's weight, trust level;

- information about attacks associated with spoofed network resources, the DNS and IP addresses (IPv4 and IPv6) of visited websites;

- DNS and IP addresses (IPv4 or IPv6) of the requested web resource, information about the file and web client accessing the web resource, the name, size and checksums (MD5, SHA2-256, SHA1) of the file, full path to the file and path template code, the result of checking its digital signature, and its status in KSN;

- information about rollback of malware actions: data on the file whose activity was rolled back (name of the file, full path to the file, its size and checksums (MD5, SHA2-256, SHA1)), data on successful and unsuccessful actions to delete, rename and copy files and restore the values in the registry (names of registry keys and their values), and information about system files modified by malware, before and after rollback;

- Information about the exclusions set for the Adaptive Anomaly Control component: the ID and status of the rule that was triggered, the action performed by the Software when the rule was triggered, the type of user account under which the process or the thread performs suspicious activity, information about the process that performed or was subject to the suspicious activity (script ID or process file name, full path to the process file, path template code, checksums (MD5, SHA2-256, SHA1) of the process file); information about the object that performed the suspicious actions and about the object that was subject to the suspicious actions (registry key name or file name, full path to the file, path template code, and checksums (MD5, SHA2-256, SHA1) of the file).

- information about loaded software modules: name, size and checksums (MD5, SHA2-256, SHA1) of the module file, full path to it and the path template code, digital signature settings of the module file, data and time of signature creation, name of the subject and organization that signed the module file, ID of the process in which the module was loaded, name of the module supplier, and the sequence number of the module in the loading queue;

- information about the quality of Software interaction with the KSN services: start and end date and time of the period when the statistics were generated, information about the quality of requests and connection to each of the KSN services used (KSN service ID, number of successful requests, number of requests with responses from cache, number of unsuccessful requests (network problems, KSN being disabled in the Software settings, incorrect routing), time spread of the successful requests, time spread of the cancelled requests, time spread of the requests with exceeded time limit, number of connections to KSN taken from cache, number of successful connections to KSN, number of unsuccessful connections to KSN, number of successful transactions, number of unsuccessful transactions, time spread of the successful connections to KSN, time spread of the unsuccessful connections to KSN, time spread of the successful transactions, time spread of the unsuccessful transactions);

- if a potentially malicious object is detected, information is provided about data in the processes' memory: elements of the system object hierarchy (ObjectManager), data in UEFI BIOS memory, names of registry keys and their values;

- information about events in the systems logs: the event's timestamp, the name of the log in which the event was found, type and category of the event, name of the event's source and the event's description;

- information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening;

- information about the date of Software installation and activation on the Computer: the ID of the partner that sold the license, the serial number of the license, the signed header of the ticket from the activation service (the ID of a regional activation center, the checksum of the activation code, the checksum of the ticket, the ticket creation date, the unique ID of the ticket, the ticket version, the license status, the ticket start/end date and time, the unique ID of the license, the license version), the ID of the certificate used to sign the ticket header, the checksum (MD5) of the key file, the unique ID of Software installation on the Computer, the type and ID of the application that gets updated, the ID of the update task;

- information about the set of all installed updates, and the set of most recently installed/removed updates, the type of event that caused the update information to be sent, duration since the installation of last update, information about any currently installed anti-virus databases;

- information about software operation on the computer: data on CPU usage, data on memory usage (Private Bytes, Non-Paged Pool, Paged Pool), number of active threads in the software process and pending threads, and the duration of software operation prior to the error;

- number of software dumps and system dumps (BSOD) since the Software was installed and since the time of the last update, the identifier and version of the Software module that crashed, the memory stack in the Software's process, and information about the anti-virus databases at the time of the crash;

- data on the system dump (BSOD): a flag indicating the occurrence of the BSOD on the Computer, the name of the driver that caused the BSOD, the address and memory stack in the driver, a flag indicating the duration of the OS session before the BSOD occurred, memory stack of driver that crashed, type of stored memory dump, flag for the OS session before BSOD lasted more than 10 minutes, unique identifier of the dump, timestamp of the BSOD;

- information about errors or performance problems that occurred during operation of the Software components: the status ID of the Software, error type, code and cause as well of the time when the error occurred, the IDs of the component, module and process of the product in which the error occurred, the ID of the task or update category during which the error occurred, logs of drivers used by the Software (error code, module name, name of the source file and the line where the error occurred);

- information about updates of anti-virus databases and Software components: the name, date and time of index files downloaded during the last update and being downloaded during the current update;

- information about abnormal termination of the Software operation: the creation timestamp of the dump, its type, the type of event that caused the abnormal termination of the Software operation (unexpected power-off, third-party application crash), date and time of the unexpected power-off;

- information about the compatibility of Software drivers with hardware and Software: information about OS properties that restrict the functionality of Software components (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), type of download Software installed (UEFI, BIOS), Trusted Platform Module (TPM) identifier, TPM specification version, information about the CPU installed on the Computer, operating mode and parameters of Code Integrity and Device Guard, operating mode of drivers and reason for use of the current mode, version of Software drivers, software and hardware virtualization support status of the Computer;

- information about third-party applications that caused the error: their name, version and localization, the error code and information about the error from the system log of applications, the address of the error and memory stack of the third-party application, a flag indicating the occurrence of the error in the Software component, the length of time the third-party application was in operation before the error occurred, checksums (MD5, SHA2-256, SHA1) of the application process image, in which the error occurred, path to the application process image and template code of the path, information from the system log with a description of the error associated with the application, information about the application module, in which an error occurred (exception identifier, crash memory address as an offset in the application module, name and version of the module, identifier of the application crash in the Rightholder's plug-in and memory stack of the crash, duration of the application session before crash);

- version of the Software updater component, number of crashes of the updater component while running update tasks over the lifetime of the component, ID of the update task type, number of failed attempts of the updater component to complete update tasks;

- information about the operation of the Software system monitoring components: full versions of the components, date and time when the components were started, code of the event that overflowed the event queue and number of such events, the total number of queue overflow events, information about the file of the process of the initiator of the event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file, file version), identifier of the event interception that occurred, the full version of the interception filter, identifier of the type of the intercepted event, size of the event queue and the number of events between the first event in the queue and the current event, number of overdue events in the queue, information about the file of the process of the initiator of the current event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file), duration of the event processing, maximum duration of the event processing, probability of sending statistics, information about OS events for which the processing time limit was exceeded (date and time of the event, number of repeated initializations of anti-virus databases, date and time of the last repeated initialization of anti-virus databases after their update, event processing delay time for each system monitoring component, number of queued events, number of processed events, number of delayed events of the current type, total delay time for the events of the current type, total delay time for all events);

- information from the Windows event tracing tool (Event Tracing for Windows, ETW) in the event of Software performance problems, suppliers of SysConfig / SysConfigEx / WinSATAssessment events from Microsoft: information about the Computer (model, manufacturer, form factor of the housing, version), information about Windows performance metrics (WinSAT assessments, Windows performance index), domain name, information about physical and logical processors (number of physical and logical processors, manufacturer, model, stepping level, number of cores, clock frequency, CPUID, cache characteristics, logic processor characteristics, indicators of supported modes and instructions), information about RAM modules (type, form factor, manufacturer, model, capacity, granularity of memory allocation), information about network interfaces (IP and MAC addresses, name, description, configuration of network interfaces, breakdown of number and size of network packages by type, speed of network exchange, breakdown of number of network errors by type), configuration of IDE controller, IP addresses of DNS servers, information about the video card (model, description, manufacturer, compatibility, video memory capacity, screen permission, number of bits per pixel, BIOS version), information about plug-and-play devices (name, description, device identifier [PnP, ACPI], information about disks and storage devices (number of disks or flash drives, manufacturer, model, disk capacity, number of cylinders, number of tracks per cylinder, number of sectors per track, sector capacity, cache characteristics, sequential number, number of partitions, configuration of SCSI controller), information about logical disks (sequential number, partition capacity, volume capacity, volume letter, partition type, file system type, number of clusters, cluster size, number of sectors per cluster, number of empty and occupied clusters, letter of bootable volume, offset address of partition in relation to the start of the disk), information about BIOS motherboard (manufacturer, release date, version), information about motherboard (manufacturer, model, type), information about physical memory (shared and free capacity), information about operating system services (name, description, status, tag, information about processes [name and PID]), energy consumption parameters for the Computer, configuration of interrupt controller, path to Windows system folders (Windows and System32), information about the OS (version, build, release date, name, type, installation date), size of page file, information about monitors (number, manufacturer, screen permission, resolution capacity, type), information about video card driver (manufacturer, release date, version);

- information from ETW, suppliers of EventTrace / EventMetadata events from Microsoft: information on the sequence of system events (type, time, date, time zone), metadata about the file with tracing results (name, structure, tracing parameters, breakdown of number of trace operations by type), information about the OS (name, type, version, build, release date, start time);

- information from ETW, suppliers of Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power events from Microsoft: information about started and completed processes (name, PID, start parameters, command line, return code, power management parameters, start and completion time, access token type, SID, SessionID, number of descriptors installed), information about changes in thread priorities (TID, priority, time), information about disk operations of the process (type, time, capacity, number), history of changes to the structure and capacity of usable memory processes;

- information from ETW, suppliers of StackWalk / Perfinfo events from Microsoft: information about performance counters (performance of individual code sections, sequence of function calls, PID, TID, addresses and attributes of ISRs and DPCs);

- information from ETW, supplier of KernelTraceControl-ImageID events from Microsoft: information on executable files and dynamic libraries (name, image size, full path), information on PDB files (name, identifier), VERSIONINFO resource data for executable files (name, description, creator, localization, application version and identifier, file version and identifier);

- information from ETW, suppliers of FileIo / DiskIo / Image / Windows Kernel Disk events from Microsoft: information on file and disk operations (type, capacity, start time, completion time, duration, completion status, PID, TID, driver function call addresses, I/O Request Packet (IRP), Windows file object attributes), information about files involved in file and disk operations (name, version, size, full path, attributes, offset, image checksum, open and access options);

- information from ETW, supplier of PageFault events from Microsoft: information on memory page access errors (address, time, capacity, PID, TID, attributes of Windows file object, memory allocation parameters);

- information from ETW, supplier of Thread events from Microsoft: information on thread creation/completion, information on threads started (PID, TID, size of stack, priorities and allocation of CPU resources, I/O resources, memory pages between threads, stack address, address of init function, address of Thread Environment Block (TEB), Windows service tag);

- information from ETW, supplier of Microsoft Windows Kernel Memory events from Microsoft: information about memory management operations (completion status, time, quantity, PID), memory allocation structure (type, capacity, SessionID, PID);

- information about Software operation in the event of performance problems: Software installation identifier, type and value of drop in performance, information about the sequence of events within the Software (time, time zone, type, completion status, Software component identifier, Software operating scenario identifier, TID, PID, function call addresses), information about network connections to be checked (URL, direction of the connection, size of network package), information about PDB files (name, identifier, image size of executable file), information about files to be checked (name, full path, checksum), Software performance monitoring parameters;

- information about the last unsuccessful OS restart: the number of unsuccessful restarts since OS installation, data on the system dump (code and parameters of an error, name, version and checksum (CRC32) of the module that caused an error in the OS operation, error address as an offset in the module, checksums (MD5, SHA2-256, SHA1) of the system dump);

- information to verify authenticity of digital certificates being used to sign files: the certificate's fingerprint, the checksum algorithm, the certificate's public key and serial number, the name of the issuer of the certificate, the result of certificate validation and the certificate's database identifier;

- information about the process executing the attack on the Software's self-defense: the name and size of the process file, its checksums (MD5, SHA2-256, SHA1), the full path to the process file and the template code of the file path, the creation/build timestamps, executable file flag, attributes of the process file, information about the certificate used to sign the process file, code of the account used to launch the process, ID of operations performed to access the process, type of resource with which the operation is performed (process, file, registry object, FindWindow search function), name of resource with which the operation is performed, flag indicating success of the operation, the status of the file of the process and its signature according to the KSN;

- information about the Rightholder's Software: full version, type, localization and operation state of Software used, versions of the installed Software components and their operation state, information about the installed Software updates, the value of the TARGET filter, the version of the protocol used to connect to the Rightholder's services;

- information about hardware installed on the Computer: type, name, model name, firmware version, parameters of built-in and connected devices, the unique identifier of the Computer with the installed Software;

- information about the versions of the operating system and installed updates, the word size, edition and parameters of the OS run mode, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, and OS startup date and time;

- executable and non-executable files, either entirely or partly;

- portions of the Computer's RAM;

- sectors involved in the process of booting the OS;

- network traffic data packets;

- web pages and emails containing suspicious and malicious objects;

- description of the classes and instances of classes of the WMI repository;

- application activity reports:
  - the name, size and version of the file being sent, its description and checksums (MD5, SHA2-256, SHA1), file format identifier, the name of the file's vendor, the name of the product to which the file belongs, full path to the file on the Computer, template code of the path, the creation and modification timestamps of the file;
  - start and end date/time of the validity period of the certificate (if the file has a digital signature), the date and the time of the signature, the name of the issuer of the certificate, information about the certificate holder, the fingerprint, the certificate's public key and appropriate algorithms, and the certificate's serial number;
  - the name of the account from which the process is running;
  - checksums (MD5, SHA2-256, SHA1) of the name of the Computer on which the process is running;
  - titles of the process windows;
  - Identifier for the anti-virus databases, name of the detected threat according to the Rightholder's classification;
  - data about the installed license, its identifier, type and expiration date;
  - local time of the Computer at the moment of the provision of information;
  - names and paths of the files that were accessed by the process;
  - names of registry keys and their values that were accessed by the process;
  - URL and IP addresses that were accessed by the process;
  - URL and IP addresses from which the running file was downloaded.

Compliance with European Union legislation (GDPR)

Kaspersky Industrial CyberSecurity for Nodes may transmit data to Kaspersky under the following scenarios:

- Using Kaspersky Security Network.
- Activating the application with an activation code.
- Updating application modules and anti-virus databases.
- Following links in the Application Console.

Irrespective of the data classification and territory from which the data is received, Kaspersky adheres to high standards for data security and employs various legal, organizational and technical measures to protect the data of users, to guarantee data security and confidentiality, and also to ensure the fulfillment of users' rights as guaranteed by applicable legislation. The text of the Privacy Policy is included in the application distribution kit and is available on the Kaspersky website.

Prior to using Kaspersky Industrial CyberSecurity for Nodes, please carefully read the description of transmitted data in the End User License Agreement and Kaspersky Security Network Statement (listed in the Kaspersky Security Network Statement). If specific data transmitted from Kaspersky Industrial CyberSecurity for Nodes under any of the described scenarios may be classified as personal data according to your local legislation or standard, you must ensure that such data is processed legally and obtain the consent of end users for the collection and transmission of such data.

Read the End User License Agreement and visit the Kaspersky website to learn more about how we receive, process, store, and destroy information about application usage after you accept the End User License Agreement and consent to the Kaspersky Security Network Statement. The license.txt and ksn_<language ID>.txt files contain the text of the End User License Agreement and Kaspersky Security Network Statement and are included in the application distribution kit.

If you do not want to transmit data to Kaspersky, you can disable data provision.

Using Kaspersky Security Network

By using Kaspersky Security Network, you agree to automatically provide the data listed in the Kaspersky Security Network Statement. If you do not agree to provide this data to Kaspersky, use Kaspersky Private Security Network (KPSN) or disable the use of KSN.

Activating the application with an activation code

By using an activation code, you agree to automatically provide the data under the End User License Agreement. If you do not agree to provide this data to Kaspersky, use a key file to activate Kaspersky Industrial CyberSecurity for Nodes.

Updating application modules and anti-virus databases

By using Kaspersky servers, you agree to automatically provide the data under the End User License Agreement. Kaspersky requires this information to verify that Kaspersky Industrial CyberSecurity for Nodes is being legitimately used. If you do not agree to provide this information to Kaspersky, use Kaspersky Security Center for database updates.

Following links in the Application Console.

By using links in the Application Console, you agree to automatically provide the data under the End User License Agreement. The precise list of data transmitted in each specific link depends on where the link is located in the Application Console and which problem it aims to resolve. If you do not agree to provide this information to Kaspersky, disable the display of the application interface.

Information about third-party code

Information about third-party code is contained in the legal_notices.txt file, located in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Pentium is a trademark of Intel Corporation or its subsidiaries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, Outlook, PowerShell, SharePoint, SQL Server, Windows, Windows Server, Windows Vista, Windows XP are trademarks of the Microsoft group of companies.

Schneider Electric is a trademark of Schneider Electric.

Siemens, Simatic, and WinCC are registered trademarks of Siemens AG.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.