kaspersky

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

© 2026 AO Kaspersky Lab

Contents

Kaspersky SIEM
About the solution
- What's new in version 4.6
- Fixed issues
- Hardware and software requirements
  - Hardware requirements
  - Software requirements
  - Requirements for Windows devices for agent installation
  - Requirements for Linux devices for agent installation
  - Requirements for devices running on Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS
  - Requirements for client devices for managing the KUMA web interface
  - Device requirements for installing KUMA on Kubernetes
  - Selecting hardware for ClickHouse cluster storages
  - EPS-dependent hardware configurations and scaling
- Distribution kit
- Architecture of the solution

Deployment and initial configuration
- Choosing a deployment configuration
  - Interaction of nodes in a Kubernetes cluster
  - Interaction of Kaspersky SIEM components with a Raft cluster
- Installation preparation
- Installation on a single server
- Installation in a distributed configuration
- Installing in a high availability configuration in a Kubernetes cluster
- Installing in a high availability configuration in a Raft cluster
- Configuring exclusions in Kaspersky Endpoint Security for Linux
- Logging in to the web interface

Administration
- Updating
  - Updating previous versions of the solution
  - Upgrading Oracle Linux 8.x to Oracle Linux 9.x with installed KUMA services
- Data back up and recovery
  - Creating a backup of the KUMA Core
  - Backing up the KUMA Core using the API
  - Restoring the KUMA Core for a single-server installation
  - Restoring the KUMA Core for a distributed installation
  - Restoring in a Kubernetes cluster
  - Restoring in a Raft cluster
- Maintenance of hosts in a Kubernetes cluster
- Modifying a previously deployed configuration
  - Expanding a single-server deployment configuration to a distributed configuration
  - Adding servers for collectors to a distributed installation
  - Adding servers for correlators to a distributed installation

- Adding servers to an existing storage cluster
- Adding another storage cluster
- Migrating the KUMA Core to a new Kubernetes cluster
- Removing a server from a distributed installation
- Deleting a storage cluster
- Expanding the Raft cluster
- Deleting a Raft cluster node
- Growing the KUMA Core volume or the Metrics service volume in an active Kubernetes cluster
- Shrinking the Metrics service volume
- Changing the host name for a single-server deployment
- Changing the host name for a distributed deployment
- Changing the hostname of the KUMA Core

Organizing a multi-tenant architecture
- Cross-tenant interaction rules
- Example of configuring multi-tenancy
- Working with tenants
- Enabling and disabling the display of tenants

Managing users and configuring access by roles
- User roles
- Rights of predefined roles
- Creating a user role
- Functional areas and permissions available to them
- Editing user role settings
- Viewing role settings
- Deleting a user role
- Configuring the security policy for logging in to the web interface
- Creating a user account
- Editing a user account
- Changing the account password
- Special considerations involved in changing the set of spaces assigned to a user

Configuring notifications
- Connecting to an SMTP server
- Standard email notifications
- Custom notification templates
  - Managing notification templates
  - Notification template syntax
- Telegram notifications

Managing certificates
- Downloading certificates
- Modifying the self-signed web interface certificate
- Reissuing internal CA certificates
- Reissuing a certificate for a specific service
- Reissuing the AI service certificate

- Auditing and monitoring solution status
  - Audit and monitoring of KUMA
  - Monitoring the status of services
    - Viewing KUMA metrics
    - KUMA metrics storage period
    - KUMA metric alert triggering conditions
    - Migrating the Metrics service to another host
  - Integrity check of KUMA files
- Uninstalling the solution
- Collecting and enriching events
  - Connect event sources
    - Kaspersky
      - Kaspersky Security Center (Administration server)
      - Kaspersky Security Center (MS SQL)
      - Kaspersky Web Traffic Security
      - Kaspersky Linux Mail Server
      - Kaspersky Secure Mail Gateway
      - Kaspersky Industrial CyberSecurity for Networks
      - Kaspersky Anti Targeted Attack Platform
      - Kaspersky Endpoint Security for Windows
      - Kaspersky Endpoint Security for Linux
    - Microsoft
      - KUMA Agent (WEC)
      - KUMA Agent (WMI)
      - Event Tracing for Windows connector
      - Microsoft 365
    - Unix and Linux
      - Auditd
      - FreeIPA
      - FreeRADIUS
      - ProFTPD
      - Vsftpd
      - HAProxy
      - Apache Tomcat
    - Network and security devices
      - IVK Kolchuga-K
      - CryptoPro NGate
      - Ideco UTM
      - McAfee Web Gateway
      - Positive Technologies Network Attack Discovery
      - Snort
      - Suricata
      - zVirt
      - ViPNet TIAS
      - Zeek IDS
      - Angie

Dallas Lock 8
Dallas Lock Unified Control Center
Database and DBMS audit systems
PostgreSQL
MariaDB Audit Plugin
Apache Cassandra
Cloud and virtual platforms
Nextcloud
Yandex Cloud
VMware vCenter
Veeam Backup & Replication
Mail and collaboration systems
CommuniGate Pro
Postfix
Sendmail
VK WorkSpace Mail
Other specialized systems
Codemaster Mirada
APKSh Kontinent
Ansible
Grafana
TeamPass
SaltStack
Monitoring event sources
Determining event sources
Viewing information about event sources
Viewing the dynamics of incoming events
Exporting event source information to a CSV file
Deleting an event source
Algorithm for applying a monitoring policy
Viewing monitoring policies
Creating a monitoring policy
Applying monitoring policies
Modifying and updating a monitoring policy
Disabling monitoring policies
Creating a monitoring policy based on an existing one
Deleting monitoring policies
Integration with other solutions
Integration with Kaspersky Security Center
Configuring Kaspersky Security Center integration settings
Adding a tenant to the list for Kaspersky Security Center integration
Removing a tenant from the list of tenants for Kaspersky Security Center integration
Creating Kaspersky Security Center connection
Editing Kaspersky Security Center connection
Deleting Kaspersky Security Center connection
Importing events from the Kaspersky Security Center database
Kaspersky Vulnerability Management integration

Kaspersky Endpoint Detection and Response integration
Importing Kaspersky Endpoint Detection and Response events using the kafka connector
Importing Kaspersky Endpoint Detection and Response events using the kata/edr connector
Configuring the display of a link to a Kaspersky Endpoint Detection and Response detection in KUMA event details
Integration with Kaspersky CyberTrace
Integrating CyberTrace indicator search
Configuring CyberTrace to receive and process requests
Creating event Enrichment rules
Integrating CyberTrace interface
Configuring event enrichment and retroscan
Integration with Kaspersky Threat Intelligence Portal
Initializing the Kaspersky Threat Intelligence Portal integration
Requesting information from Kaspersky Threat Intelligence Portal
Viewing information from Kaspersky Threat Intelligence Portal
Updating information from Kaspersky Threat Intelligence Portal
Integration with R-Vision Security Orchestration, Automation and Response
Configuring integration in KUMA
Adding the ALERT_ID and ALERT_URL incident fields
Creating a collector in R-Vision SOAR
Creating connector in R-Vision SOAR
Creating rule for closing KUMA alert when R-Vision SOAR incident is closed
Configuring integration in R-Vision SOAR
Managing alerts using R-Vision SOAR
Integration with Active Directory, Active Directory Federation Services and FreeIPA
Establishing a LDAP connection to Active Directory
Enabling and disabling LDAP integration
Adding a tenant to the LDAP server integration list
Creating an LDAP server connection
Creating a copy of an LDAP server connection
Changing an LDAP server connection
Changing the data update frequency
Changing the data storage period
Starting account data update tasks
Deleting an LDAP server connection
Authentication using domain accounts
Enabling and disabling domain authentication
Configuring connection between KUMA and Active Directory
Configuring connection between KUMA and Active Directory Federation Services
Configuring connection between KUMA and FreeIPA
Managing links between roles and domain user groups
NCIRCC integration
Integration with the Security Orchestration Automation and Response Platform (SOAR)
Configuring integration in KUMA
Configuring integration in SOAR
Importing and configuring a connector
Configuring the handler, schedule, and worker process

Integration with KICS for Networks and KATA
Configuring integration in KICS for Networks or KATA
Configuring integration in KUMA
Enabling and disabling integration with KICS for Networks or KATA
Changing the data update frequency
Special considerations when importing asset information from KICS for Networks or KATA
Changing the status of a KICS for Networks or KATA asset
Kaspersky Automated Security Awareness Platform
Creating a token in ASAP and getting a link for API requests
Configuring integration in KUMA
Viewing information about the users from ASAP and changing learning groups
UserGate integration
Configuring integration in UserGate
Preparing a script for integration with UserGate
Configuring a response rule for integration with UserGate
Integration with Kaspersky Web Traffic Security
Configuring integration in KWTS
Preparing a script for integration with KWTS
Configuring a response rule for integration with KWTS
Integration with Kaspersky Secure Mail Gateway
Configuring integration in KSMG
Preparing a script for integration with KSMG
Configuring a response rule for integration with KSMG
Kaspersky Managed Detection and Response integration
Preliminary configuration
Initializing integration
Importing asset information from RedCheck
Storing events
About the ClickHouse cluster
Creating a storage
Viewing the storage partitions
Viewing active queries in ClickHouse
Cold storage of events
Removing cold storage disks
Disconnecting, archiving, and connecting partitions
Scheduling partition backup
Manually backing up partitions
Restoring partitions from backup
Importing partitions from a third-party instance of Kaspersky SIEM
Configuring retention periods and priority deletion of events
Event reception and normalization
Algorithm of collector operation
Supported event sources
Creating a collector
Installing the collector on the server
Ensuring uninterrupted collector operation
Event aggregation

Normalization of events
Generating regular expressions with KIRA
Configuring extra normalization of events
Reusing normalizers
Using an extended event scheme for normalization
Viewing the table of extended event schema fields
Adding, modifying, and deleting fields of the extended event schema
Importing and exporting extended event schema fields
Using the connector
Connector settings
Connector, internal type
Connector, tcp type
Connector, udp type
Connector, netflow type
Connector, sflow type
Connector, nats-jetstream type
Connector, kafka type
Connector, http type
Connector, sql type
Connector, file type
Connector, 1c-log type
Connector, 1c-xml type
Connector, diode type
Connector, ftp type
Connector, sftp type
Connector, nfs type
Connector, wmi type
Connector, wec type
Connector, etw type
Connector, snmp type
Connector, snmp-trap type
Configuring the source of SNMP trap messages for Windows
Configuring and starting the SNMP and SNMP trap services
Configuring the Event to Trap Translator service
Connector, kata/edr type
Connector, vmware type
Connector, elastic type
Connector, office365 type
Connector, dfi type
Connector, universalAPI type
Connector, smb type
Predefined connectors
Using a destination
Destination, internal type
Destination, type nats-jetstream
Destination, tcp type
Destination, udp type

- Destination, http type
- Destination, diode type
- Destination, kafka type
- Destination, file type
- Destination, storage type
- Destination, correlator type
- Destination, eventRouter type
- Using a proxy server
- Using the dictionary
- Configuring detection logic and correlation rules
- Algorithm of correlator operation
- Creating a correlator
- Creating a correlator NG
- Supported data types for correlator NG
- Correlation rule selectors and expressions
- Data processing functions in correlator NG
- Installing the correlator on the server
- Correlation rules
- Working with correlation rules
- Correlation rules of the 'standard' type
- Correlation rules of the 'simple' type
- Correlation rules of the 'operational' type
- Using filters in correlation rules
- Limiting how many times a correlation rule can be triggered
- Variables in correlators
- Local variables in identical and unique fields
- Local variables in selector
- Local Variables in event enrichment
- Local variables in active list enrichment
- Properties of variables
- Requirements for variables
- Functions of variables
- Declaring variables
- Adding a temporary exclusion list for a correlation rule
- Predefined correlation rules
- Correlation rule packages
- Correlation using assets and asset categories
- MITRE ATT&CK techniques and tactics
- Importing the list of MITRE ATT&CK techniques
- Adding MITRE enrichment rules to the correlator
- Mapping MITRE ATT&CK techniques to correlation rules
- Exporting correlation rules to MITRE ATT&CK Navigator
- Sigma rules converter
- Converting and uploading Sigma rules
- Examples of supported Sigma rule conversions

- Segmentation rules
  - Creating a segmentation rule
  - Linking segmentation rules to correlation rules
- Active lists
  - Viewing the table of correlator active lists
  - Adding active list
  - Viewing the settings of an active list
  - Changing the settings of an active list
  - Duplicating an active list
  - Deleting active lists
  - Viewing records in the active list
  - Searching for records in the active list
  - Adding a record to an active list
  - Duplicating records in the active list
  - Changing a record in the active list
  - Deleting records from the active list
  - Import entries to an active list
  - Exporting records from the active list
  - Predefined active lists
- Context tables
  - Viewing the list of context tables
  - Adding a context table
  - Viewing context table settings
  - Editing context table settings
  - Duplicating context table settings
  - Deleting a context table
  - Viewing and finding records in the context table
  - Adding, editing, and deleting records in the context table
  - Exporting data from a context table
  - Importing data into a context table

Event enrichment
- Viewing the enrichment rules
- Creating enrichment rule
- Linking the enrichment rules
- Managing enrichment rules
- Adding enrichment rules in collector properties
- Enriching events with assets
- Enriching events with geodata
  - Geodata format
  - Converting geographic data from MaxMind to IP2Location
  - Importing and exporting geographic data
  - Default mapping of geographic data
- Enriching events with data from Active Directory
- Enriching events with DNS names
- Enriching events using a dictionary

Event routing
Starting the Event Router Installation Wizard
Step 1. General settings of the event router
Step 2. Routing
Step 3. Setup validation
Installing the event router on the server
Use case: the collector sends events to a router in a data center
Use case: cascade of event routers
Creating and using KUMA agents
Creating a set of resources for an agent
Managing connections for an agent
Creating an agent service in the KUMA web interface
Automatically created agents
Installing an agent in a KUMA network infrastructure
Installing a KUMA agent on Linux assets
Installing a KUMA agent on Windows assets
Update agents
Transferring events from isolated network segments to KUMA
Diode agent configuration file
Description of secret fields
Installing Linux Agent in an isolated network segment
Installing Windows Agent in an isolated network segment
Configuring an agent to receive NetFlow events from an isolated segment
Getting service data about events from an isolated segment
Receiving sensitive data over an encrypted connection
Transferring events from Windows computers to KUMA
Importing a file with a list of servers for WMI agents
Managing assets
Adding an asset category
Configuring the table of assets
Searching assets
Exporting asset data
Viewing asset details
Adding assets
Adding asset information in the KUMA web interface
Importing asset information and asset vulnerability information from Kaspersky Security Center
Importing asset information from MaxPatrol
Importing data from MaxPatrol reports
Importing asset information from MaxPatrol VM
Settings of the kuma-ptvm-config.yaml configuration file
Settings in the kuma-ptvm-vulnerable-assets-config-template.yaml configuration file
Importing asset information from KICS for Networks
Examples of asset field comparison during import
Working with Kaspersky Security Center tasks
Creating KUMA tasks in Kaspersky Security Center
Starting Kaspersky Security Center tasks manually

- Starting Kaspersky Security Center tasks automatically
- Checking the status of Kaspersky Security Center tasks
- Assigning a category to an asset
- Editing the parameters of assets
- Archiving assets
- Deleting assets
- Bulk deletion of assets
- Updating third-party applications and fixing vulnerabilities on Kaspersky Security Center assets
- Moving assets to a selected administration group
- Asset audit
  - Configuring an asset audit
  - Storing and searching asset audit events
  - Enabling and disabling an asset audit
- Detection of unknown assets
- Custom asset fields
- Critical information infrastructure assets
- Storing confidential information (secrets)
- Working with the knowledge base
- Managing resources and services
  - General instructions for working with resources
    - Creating, duplicating, moving, editing, and deleting resources
    - Linking resources to services
    - Updating predefined resources
    - Exporting resources
    - Importing resources
    - Resource search
  - Viewing Kaspersky SIEM services
  - General instructions for working with services
  - Versioning of resources and services
  - Viewing a dependency graph
  - Tag management
  - Managing folders
- Analyzing data and working with security incidents
  - Security monitoring
    - Dashboards
      - Predefined dashboards
      - Availability of dashboards in different tenants
      - Dashboard management
      - Selecting a dashboard
      - Enabling and disabling the TV mode
      - Selecting the period without modifying dashboard settings
      - Exporting dashboards
      - Importing dashboards
    - Reports
      - Availability of report templates across different tenants
      - Viewing generated reports
      - Viewing report templates

- Creating report template
- Managing report templates
- Exporting and importing report templates
- Managing reports
- Configuring report schedule
- Saving a report
- Widgets
  - Basics of managing widgets
  - Special considerations for displaying data in widgets
  - Managing widgets
  - Widget settings
    - Events widget
    - Active lists widget
    - Context tables widget
    - Assets custom widget
    - Image widget
    - Text widget
    - Other widgets
  - Filtering widget data
    - Filtering data on a single widget
    - Filtering data in multiple widgets
    - Drilling down to a related dashboard
  - Displaying tenant names in Active list type widgets
- Response
  - Response rules for Kaspersky Security Center
  - Response rules for a custom script
  - Response rules for KICS for Networks
  - Response rules for Kaspersky Endpoint Detection and Response
  - Active Directory response rules
  - Response rules with EDR actions
- Working with events
  - Event life cycle
  - Filtering and searching events
    - Selecting Storage
    - Generating an SQL query using a builder
    - Manually creating an SQL query
    - Building a process chain using an SQL query
    - Saving query history
    - Managing saved search queries
    - Searching for related events
    - Searching for events using account and asset information
    - Filtering events by time range
    - Displaying the list of events with a relative and absolute calendar period
    - Grouping events
    - Displaying names instead of IDs
    - Presets
    - Limiting the complexity of queries in alert investigation mode

Saving and selecting events filter configuration
Deleting event filter configurations
Supported ClickHouse functions
Viewing event detail areas
Exporting events
Configuring the table of events
Refreshing events table
Getting events table statistics
Viewing correlation event details
Generating an SQL query using KUMA SQL functions
Using the 'enrich' function set in SQL queries
Using the 'lookup' function set in SQL queries
Data collection and analysis rules
Managing data collection and analysis rules
Configuring the scheduler for a data collection and analysis rule
Analyzing network traffic volume
Retroscan
Event route tracing
Categorization of events
Granular access to events
Managing sets of spaces
Scenarios for using granular access to events
Working with alerts
Severity
Configuring alerts table
Filtering alerts
Saving and selecting an alert filter
Deleting an alert filter
Viewing alert details
Changing alert name
Configuring alert filling
Processing alerts
Alert investigation
Retention of alerts and incidents
Alert notifications
Working with incidents
Viewing incidents
Saving and selecting incident filter configuration
Deleting incident filter configurations
Viewing incident details
Incident creation
Incident processing
Changing incidents
Automatic linking of alerts to incidents
Categories and types of incidents

- Interaction with NCIRCC
  - Exporting data to NCIRCC
  - Getting incidents from NCIRCC
  - Supplementing incident data on request
  - Sending files to NCIRCC
  - Communication with NCIRCC experts
  - Supported categories and types of NCIRCC incidents
  - Notifications about the incident status change in NCIRCC
- Example of incident investigation using Kaspersky SIEM
  - Incident conditions
  - Step 1. Preliminary steps
  - Step 2. Assigning an alert to a user
  - Step 3. Check if the triggered correlation rule matches the data of the alert events
  - Step 4. Analyzing alert information
  - Step 5. False positive check
  - Step 6. Determining alert severity
  - Step 7. Incident creation
  - Step 8. Investigation
  - Step 9. Searching for related assets
  - Step 10. Searching for related events
  - Step 11. Recording the causes of the incident
  - Step 12. Incident response
  - Step 13. Restoring assets operability
  - Step 14. Closing the incident
- AI services
  - AI score and status of assets
    - Installing and removing the AI asset score and status service
    - Settings of the AI asset score and status service
  - Using the KIRA AI Assistant
    - Configuring integration with KIRA using KSN
    - Configuring integration with KIRA using an LLM provider
    - Analyzing using KIRA
  - DLL Hijacking attack detection
- Working with the task manager
  - Viewing the tasks table
  - Configuring the display of the tasks table
  - Viewing task run results
  - Restarting a task
Troubleshooting
- Known issues and limitations
- Contact Technical Support
- KUMA logs
- Port check
- Resolving the problem of insufficient disk space
- Fixing the "Access denied" error when logging in to KUMA via AD FS
- Reissuing k0s cluster certificates upon expiration

Resolving the DB::Exception error when updating KUMA
Merging duplicate assets
REST API
Creating a token
Configuring permissions to access the API
Authorizing API requests
Standard error
Appendices
KUMA settings in the inventory file
Configuring the KUMA Core
Commands for components manual starting and installing
Ports used by KUMA during installation
Network settings for interaction with external services
Normalized event data model
Configuring the data model of a normalized event from KATA EDR
Alert data model
Asset data model
User account data model
KUMA audit events
User was successfully signed in or failed to sign in
User login changed
Other data of the user was changed
User logged out
User password was changed
User was created
User role was assigned
User role was revoked
The user has edited the set of fields settings to define sources
Alert assigned to the user
User access token was changed
Key file added
Application activated with an activation code
Reserve license key added
Reserve license key deleted
The license is renewed
Invalid activation code
Activation code blocked
Activation code or key file deleted
Activation code or key file replaced
EPS exceeded
License expiration and start of grace period
End of grace period
Expired activation code or key file added
Changed the set of spaces to differentiate access to events
Service monitoring thresholds changed
KUMA Core settings modified
GeoIP databases imported

Service was created
Service was deleted
Service was reloaded
Service was restarted
Service was started
Service was paired
Service status was changed
Partition was deleted by user
Partition automatically deleted after retention period
Partition deleted by absolute retention period
Partition deleted by relative retention period
Partition moved to cold storage
Error moving partition to cold storage
Active list was successfully cleared or operation failed
Active list item was successfully changed, or operation was unsuccessful
Active list item was successfully deleted or operation was unsuccessful
Active list was successfully imported or operation failed
Active list was exported
Context table exported
Context table successfully imported or operation failed
Context table item successfully modified or operation failed
Context table item modified or operation failed
Context table successfully cleared or operation failed
Resource was added
Resource was deleted
Resource was updated
Importing resources
Asset was created
Asset was deleted
Asset category was added
Asset category was deleted
Settings were updated
Tenant was created
Tenant was enabled
Tenant was disabled
Other tenant data was changed
The dictionary was successfully updated on the service or operation was unsuccessful
Dictionary entry added
Dictionary entry successfully deleted or the operation failed
Incident successfully created or operation failed
Incident successfully closed or operation failed
Incident assigned to a user or operation failed
Alert linked to an incident or alert unlinked from an incident, or operation failed
Metrics alert registered for service or operation failed
Event linked to an alert or unlinked from an alert, or operation failed
Response in Active Directory
Extended event schema field created

Extended event schema field edited
Extended event schema field imported
Normalizer with extended event schema field imported
Extended event schema field deleted
Query sent to KIRA
KICS/KATA response
Kaspersky Automated Security Awareness Platform response
KEDR response
Importing MITRE ATT&CK techniques and tactics
Backing up KUMA Core and restoring from backup
Backing up partitions, restoring from backup, importing partitions from an external KUMA installation
Attempt to read events
The search request has been canceled
Exporting resources from KUMA
Rule is linked to the collector
Rule is unlinked from the collector
Rule is linked to the correlator
Rule is unlinked from the correlator
Filters
Sending test events to KUMA
Time format
Mapping fields of predefined normalizers
Deprecated resources
Generating events for testing a normalizer
Legal information
Licensing the solution
Viewing the End User License Agreement
License groups and merged license
Managing license keys in the KUMA web interface
Data provision
Compliance with European Union legislation (GDPR)
Information about third-party code
Trademark notices
The MITRE Corporation Terms of Use

Kaspersky SIEM

Solution overview

About the solution

What's new in version 4.6

Hardware and software requirements

Architecture

Getting started

Choosing a deployment configuration

Installation preparation

Deployment and initial configuration

Logging in to the solution web interface

Administrator's guide

Integrity check

Updating

Data back up and recovery

Modifying a previously deployed configuration

Organizing a multi-tenant architecture

Managing users and configuring access by roles

Auditing and monitoring solution status

User guide

Collecting and processing events

Connect event sources

Managing assets

Integration with other solutions

Storing events

Event reception and normalization

Configuring detection logic and correlation rules

Event enrichment

Analyzing data and working with security incidents

Example of incident investigation

Security monitoring

Response

Working with events

Working with alerts

Working with incidents

Using AI services

About the solution

Kaspersky Unified Monitoring and Analysis Platform (hereinafter also referred to as KUMA, or Kaspersky SIEM, or "solution") is a SIEM class solution designed for centralized collection, storage, and analysis of information security events. The solution helps to detect suspicious activity and security incidents. It provides data visualization capabilities, enables you to generate automated reports, and delivers analytical support for monitoring and investigation processes within an organization's infrastructure.

The solution is built on a microservice architecture. The functionality of KUMA is implemented as separate services that can be deployed and configured independently of each other. This allows you to change the solution configuration depending on the characteristics of the organization's infrastructure, to scale event processing, and to ensure system fault tolerance.

Available functionality:

Real-time correlation and correlation based on indexed data

Kaspersky SIEM provides centralized collection and analysis of information security events, real-time event correlation, and timely incident notifications, while allowing to analyze accumulated data and group, aggregate, normalize, and correlate such data using data mining rules.

Integration with Kaspersky Threat Intelligence

The Kaspersky SIEM solution is tightly integrated with the Kaspersky Threat Intelligence portfolio of services. Integration with Kaspersky CyberTrace allows using threat data feeds for scanning and use enriched data for correlation and search queries. Integration with the Kaspersky Threat Intelligence Portal (Threat Lookup) lets you get contextual information on new attacks, indicators of compromise, and tactics and techniques used by attackers.

Dashboards

Dashboards allow monitoring the network security status; dashboards are flexibly configurable sets of widgets that display various security data analytics.

Asset inventory and incident response

Kaspersky SIEM implements automatic collection of inventory information (installed software, vulnerabilities, hardware, asset owner), which can be used to correlate information security events based on context and during incident investigation. The ability to manage agents installed on endpoints helps in the process of responding to detected incidents.

Integration with Kaspersky Investigation and Response Assistant (KIRA)

Kaspersky SIEM supports integration with Kaspersky Investigation and Response Assistant (KIRA), an LLM tool for investigating and prioritizing alerts. KIRA performs deobfuscation of the command line output, generates a detailed analysis with a brief summary for prompt decision-making, reduces the number of errors in incident handling, lowers the requirements for the qualifications of front-line analysts, and reduces the time spent by administrators on analyzing events.

Retroscan

In addition to real-time event analysis, Kaspersky SIEM allows applying correlation rules to events that have occurred previously. This can be useful for fine-tuning correlation rules, as well as for retrospective analysis of the collected data.

The solution is not intended for distribution in the United States. Solution functionality (including anti-virus signature updates and code base updates) might not be available when the application is used on the USA territory.

What's new in version 4.6

Kaspersky Unified Monitoring and Analysis Platform 4.6.1 introduces the following features and improvements:

- You can now import resources from the repository in the **Knowledge base** section. This operation is no longer available in the resource import window.

Kaspersky Unified Monitoring and Analysis Platform 4.6 introduces the following features and improvements:

- To receive NetFlow events from an isolated network segment, a dedicated agent installed within this segment is used. The agent acts as an intermediate node: it receives NetFlow events locally and forwards them to the collector where the NetFlow connector is configured.
- Service data about events can now be sent to the collector from an isolated network segment using a dedicated agent installed inside this segment.
- Now you can set up integration with Kaspersky Vulnerability Management. When this integration is configured, Kaspersky Vulnerability Management provides KUMA with information about vulnerabilities found on assets, as well as the list of applications installed on assets. The resulting data allows timely identification and response to threats.
- Reduced load on DNS servers during DNS enrichment: the solution makes two enrichment attempts when an event occurs. After contacting the DNS server, the collector caches information about the IP address and host name on disk. This data is used for the entire retention period of the cached record. The event record is stored on disk until the cache or record is deleted from the DNS server.
- KUMA can now be installed on Red Hat Enterprise Linux 9.8.
- The list of supported operating systems on which KUMA can be installed has been updated. The minimum Linux kernel version on target hosts is now 5.15.
- Two new connectors have been added for transferring log files using SMB and SFTP.
- The list of supported event sources that KUMA can normalize has been updated.
- Now you can select a theme for the web interface of the solution. A light and a dark theme are available.
- Now you can limit the number of events added to one alert using the new **Maximum number of events** setting in the alert filling settings.
- Now you can enable compact display of `DeviceCustom*` and `Flex*` fields in the event card, in which mode the values of the `*Label` fields are displayed as field names.
- Now you can configure KIRA integration using a third-party LLM provider (the **Custom** mode).
- Now, in a normalizer with the **regexp** parsing method, you can generate regular expressions based on added examples by clicking the **Generate regular expression with KIRA** button. This automatically adds generated regular expressions to the **Normalization** field.
- A new conversion type, hexToDecimal, has been added, which allows converting values of raw event fields from hexadecimal to decimal before writing to the KUMA event fields.
- A new conversion type, unicodeUnescape has been added, which allows converting the values of raw event fields from a Unicode string to human-readable text before writing to the KUMA event fields.
- Added SQL query autocompletion. In the SQL query field, when you enter a function name, a list of available functions is displayed, and a usage example is displayed for the selected function.
- Resources from the repository are imported from the repository in the language specified in the **KUMA resources localization** setting in the KUMA Core settings section.
- ODBC SQL connectors are now supported for databases using the ODBC driver.

- The new `log_archive_setup.py` tool helps ensure compliance with European Union law (GDPR) by archiving, hashing, encrypting, verifying and deleting open data.

- New button for testing the connection to the SMTP server. To test the connection, KUMA sends a test message to the email address specified in the current user profile.

- Using the new parameters of the GET alerts/stream API method, you can limit the number of alert-related events when downloading alerts to a third-party IRP system.

- A new optional argument, `--pair.fingerprint`, helps improve the security of the connection of services to the KUMA Core. Starting with KUMA 4.6, when you create services, the installation wizard includes the KUMA Core certificate fingerprint in the installation command by default. For example: `/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:7210 --pair.fingerprint XXXX --id YYYY --api.port ZZZZ --install`. If you do not want to use authentication with a fingerprint, you can enter `insecure` as the value of the option. When upgrading from KUMA 4.2 to 4.6, no additional action is required. Services installed prior to KUMA 4.6 use the `insecure` value by default after the upgrade. If the KUMA Core certificate fingerprint is used for the `--pair.fingerprint` option, after the CA certificate is reissued, you need to copy the new fingerprint from the web interface and restart the services, updating the option with the new value in the systemd configuration. Downloadable certificates have been moved from the user profile to the **Resources and services** → **Active services** section → menu (⋮). Certificates can be downloaded if the check box next to the KUMA Core service is selected.

- Now you can import assets from MaxPatrol VM with extra filtering criteria. In the `kuma-ptvm-vulnerable-assets-config.yaml` configuration file, parameters are available for filtering assets by group, status, and severity of vulnerabilities (groups, statuses, severities).

- New access level, "Read", when managing storage partitions.

- Added a new **Knowledge Base** section for managing KUMA packages and resources. In this section, you can search and filter packages and resources, view information about them, install whole packages or individual resources, update resources, and view the dependencies between resources. KUMA 4.6 is not backward compatible with a repository of KUMA 2.1–4.2. All packages for KUMA 4.6 are new and their numbering starts with "1".

- Correlation rules of the 'periodical' type and the detection of unauthorized use of accounts, which have been added in KUMA 4.2 as beta versions, are not available in KUMA 4.6. We plan to further develop and release these functions in the next version of KUMA.

Fixed issues

The table below lists the issues found in previous versions of KUMA and fixed in version 4.6.1.

First affected version	Issue ID	Description of the issue
4.6	10611374	An audit event for a monitoring policy violation was sent to all tenants. Now such an event is sent to the tenant of the event source and to the Main tenant.
4.6	10472545	In the Knowledge Base, the filter by package status was missing the *Update required* status.
4.6	10559010	Fixed the issue that prevented services from starting after completing the deployment of KUMA with `deploy_example_services: true`.
4.6	10615952	Fixed the issue that, after upgrading from the previous version of KUMA, allowed users to edit resources imported from the repository.
4.6	10561371	Fixed the issue that caused a syntax error when using the `=` and `!=` operators when creating a search query using the builder.

4.6	10611491	Fixed the issue that caused the bars for the current and previous periods to be displayed in the same color in widgets of the Bar chart type when the **Show data for previous period** option was enabled.
4.6	10615935	Fixed the issue that prevented fields from being copied to the table in a normalizer of the **regexp** type when clicking the **Copy field names to the mapping table** button if the regular expressions were large.
4.6	10632799	Fixed an issue that prevented an alert notification from being sent to the email address.
4.6	10616043	Fixed the issue that prevented sorting by resource version in the Knowledge Base.
4.6	10616015	Fixed the issue that prevented sorting by package status in the Knowledge Base.
4.6	10665570	Fixed the issue that prevented saving information about an added certificate in the KIRA integration settings section.
4.6	10669881	Fixed an issue that caused segmentation rules with grouping by an empty field to work incorrectly. As a result, the segmentation rule would not trigger and one alert would be created.

The table below lists the issues found in previous versions of KUMA and fixed in version 4.6.

First affected version	Issue ID	Description of the issue
4.2	9398599	Fixed the issue with editing event backup that already has been configured: replicas can be overridden.
4.2	9609746	Fixed the issue with repeated email messages with reports getting sent.
4.2	9729583	Fixed an issue with sending alert notifications if multiple notification templates with different email addresses are assigned to the same correlation rule.
4.2	9731153	When getting information about incidents via the API, /api/v3/incidents/id/, the tenantName field contains the name of the tenant.
4.2	9598863	When disconnecting a cold storage disk, data deletion is performed granularly, at the part level, not at the partition level.
4.2	9773491	Changes to the list of assignments on the agent are applied correctly. Previously, the system suggested updating the configuration, but the changes would be applied only after a restart of the service.
4.2	9778401	Fixed an issue with synchronization of days of the week.
4.2	9809551	An environment variable has been added to allow uploading large files with GeoIP data.
4.2	9844469	Fixed an issue that could "freeze" the task for importing assets from Kaspersky Security Center.
4.2	10202555	The Categorized assets category can now be renamed.
4.2	9784480	The performance of the retrospective scan functionality has been optimized.
4.2	10235558	The Core service is backed up without blocking access to the service.
3.4	8306381	The algorithm for storing cached data has been changed for DNS enrichment.
4.2	9772902	Fixed issues with the sFlow normalizer.
4.2	10037706	The user interface allows using 6 or more browser tabs.
4.2	9989939	Fixed an issue with event source discovery.

Hardware and software requirements

This section describes the hardware and software requirements.

Hardware requirements

This article lists the hardware requirements for installing KUMA components depending on the EPS (events per second) received by KUMA.

The configuration of the equipment must be chosen based on the system load profile. Installation on a single server is possible with a flow of events below 10,000 EPS and if only native dashboards of the system are used.

KUMA supports Intel and AMD CPUs with SSE 4.2 and AVX instruction set support.

When deploying KUMA in a Kubernetes cluster, devices must satisfy the hardware requirements for the nodes included in the solution configuration.

The table below lists the hardware requirements for installing the KUMA components, assuming that the ClickHouse cluster only accepts INSERT queries. Hardware requirements for SELECT queries are calculated separately for the particular database usage profile of the customer.

Deploying KUMA on a single server

Hardware requirements for installing KUMA components

	Up to 3,000 EPS	Up to 10,000 EPS
Server requirements:	At least 16 threads or 16 vCPUs. At least 32 GB of RAM. At least 500 GB in the /opt directory. Data storage type: SSD. Data transfer rate: at least 100 Mbps.	At least 24 threads or 24 vCPUs. At least 64 GB of RAM. At least 500 GB in the /opt directory. Data storage type: SSD. Data transfer rate: at least 100 Mbps.
Event router requirements	–	CPU: 3 cores RAM: 240 MB.

Distributed deployment of KUMA

Hardware requirements for installing KUMA components

	Up to 20,000 EPS	Up to 50,000 EPS
KUMA Core requirements	One device. Device characteristics: • At least 12 threads or vCPUs. • At least 12 GB of RAM. • At least 500 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 53 Mbps.	One device. Device characteristics: • At least 16 threads or vCPUs. • At least 24 GB of RAM. • At least 1 TB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 134 Mbps.

	Up to 20,000 EPS	Up to 50,000 EPS
Collector requirements	One device. Device characteristics: • At least 16 threads or vCPUs. • At least 24 GB of RAM. • At least 500 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 53 Mbps.	Two devices. Characteristics of each device: • At least 16 threads or vCPUs. • At least 24 GB of RAM. • At least 500 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 134 Mbps.
Correlator requirements	One device. Device characteristics: • At least 16 threads or vCPUs. • At least 32 GB of RAM. • At least 500 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 53 Mbps.	One device. Device characteristics: • At least 16 threads or vCPUs. • At least 32 GB of RAM. • At least 500 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 134 Mbps.
Event router requirements	CPU: 6 cores RAM: 250 MB.	CPU: 9 cores RAM: 7000 MB.
Keeper requirements	Three devices. Characteristics of each device: • At least 6 threads or vCPUs. • At least 12 GB of RAM. • At least 100 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 53 Mbps.	Three devices. Characteristics of each device: • At least 6 threads or vCPUs. • At least 12 GB of RAM. • At least 100 GB in the /opt directory. • Data storage type: SSD. • Data transfer rate: at least 134 Mbps.
Storage requirements	Two devices. Characteristics of each device: • At least 24 threads or vCPUs. • At least 64 GB of RAM. • At least 16.5 TB in the /opt directory. • Data storage type: SSD*. The recommended transfer rate between ClickHouse nodes is at least 10 Gbps if the data stream is equal to or exceeds 20,000 EPS.	Four devices. Characteristics of each device: • At least 24 threads or vCPUs. • At least 64 GB of RAM. • At least 41.3 TB in the /opt directory. • Data storage type: SSD*. The recommended transfer rate between ClickHouse nodes is at least 10 Gbps if the data stream is equal to or exceeds 20,000 EPS.

Metrics service

The Metrics service monitors the performance of KUMA (the **Metrics** section) and monitors event streams from event sources (the **Source status** section).

The following parameters affect the computation resource requirements of the Metrics service:

- The total number of created KUMA services
- The settings of the event source monitoring service

The system workload profile must be considered when choosing the hardware configuration of the Metrics service.

Recommended hardware for the Metrica service

Sizing the solution depending on the number of services

The table below provides server hardware requirements for the Metrics service, depending on the number of services in the KUMA instance. The figures were calculated for an event stream of 20,000 EPS. The number of CPUs and the amount of RAM in the table are rounded up to the nearest integer number.

The results in the table were obtained with the following parameters:

- Source discovery settings: default.
- Monitoring policy settings:
  - **Type**: byCount
  - **Lower limit**: 10
  - **Upper limit**: 1000
  - **Count interval**: 10 minutes
  - **Evaluation interval**: 5 minutes

Sizing the solution depending on the number of services

Number of services	Number of CPUs (recommended)	RAM (GB) (recommended)
50	1	3
100	1	3
500	1	4

According to the table, the increase in the number of services in the KUMA instance only slightly increases the hardware requirements.

Sizing the solution depending on the event source status

The hardware requirements (CPUs, RAM, and disk space) are affected by the following parameters displayed or set in the **Metrics** and **Source status** sections:

- Settings of event source detection

  The hardware requirements are affected by the settings specified for event source detection: the number of fields and their properties. If you increase the number of fields or specify fields that contain a large number of unique values, this may result in KUMA detecting a large number of event sources. Therefore, increasing the number of event sources increases the hardware requirements.

  For example, the set of fields `DeviceProduct, DeviceHostName, DeviceAddress` detects the firewall `Firewall, fw-1.example.com, 192.0.2.1` as an event source. However, if you specify the set of fields `DeviceProduct, DeviceHostName, DeviceAddress, Name`, KUMA detects a much larger number of event sources:

  - `Firewall, fw-1.example.com, 192.0.2.1, DNS`
  - `Firewall, fw-1.example.com, 192.0.2.1, IPS`

- `Firewall, fw-1.example.com, 192.0.2.1, TRAFFIC`
- `Firewall, fw-1.example.com, 192.0.2.1, TREAT`

Consider that a noticeable impact on hardware requirements begins at 100,000 event sources.

- The number of event sources to which monitoring policies have been assigned, as well as the data counting period and the evaluation interval

  KUMA periodically receives and records information about the data feed from each event source to which a monitoring policy has been assigned with a frequency specified in the policy.

- Number of monitoring policies assigned to each event source

- Average data point size (value of the **Bytes per point** metric)

  Using the value of the **Bytes per point** (bpp) metric of the Metrics service, you can calculate how much disk space you need to store the metrics. To do this, you can use the following formula:

  ```
  hdd_sizing = ROUNDUP (bpp * (retention_sec/interval_sec) * EPS * 1.1)
  ```

  where:

  - `hdd_sizing` is the required amount of disk space
  - `ROUNDUP` is the rounding up function
  - `bpp` is the value of the **Bytes per point** metric
  - `retention_sec` is the metrics retention period in seconds
  - `interval_sec` is the information retrieval interval, equal to 15 seconds
  - `EPS` is the average EPS across sources, approximately equal to the value of the **Processing EPS** metric on the collector
  - 1.1 is a factor of safety that adds 10% to the calculated disk space.

- The stream of events processed by all collectors in KUMA

  The following table provides the hardware requirements for sizing the solution, depending on the number of event sources and monitoring policies in a KUMA instance.

  According to the table, the hardware requirements substantially increase when the number of event sources is large and a large number of monitoring policies is assigned to event sources. This data is listed in the bottom of the table.

  The results in the table were obtained with the following parameters:

  - Source discovery settings: default.
  - Monitoring policy settings:
    - **Type**: byCount
    - **Lower limit**: 10
    - **Upper limit**: 1000

- **Count interval**: 10 minutes
- **Evaluation interval**: 5 minutes

Sizing the solution depending on the number of event sources and monitoring policies

Number of event sources	Number of event sources monitored by monitoring policies	EPS	Number of monitoring policies per source	Number of CPUs (recommended)	RAM (GB) (recommended)	Disk space (GB) for 30 days of metrics retention
10,000	0	25,000	0	1	2	13
25,000	0	25,000	0	1	2	13
50,000	0	25,000	0	1	3	13
100,000	0	25,000	0	1	3	14
250,000	0	25,000	0	1	3	13
500,000	0	25,000	0	1	5	13
1,000,000	0	25,000	0	1	7	11
10,000	2000	5000	1	1	3	4
10,000	5000	5000	1	1	3	5
10,000	2000	10,000	1	1	3	8
10,000	2000	10,000	2	1	3	10
10,000	5000	10,000	1	1	3	9
10,000	5000	25,000	1	1	3	24
10,000	10,000	5000	1	1	4	5
10,000	10,000	5000	2	1	5	5
50,000	10,000	5000	1	1	4	4
50,000	10,000	10,000	1	1	5	7
50,000	25,000	25,000	1	1	6	20
100,000	20,000	5000	1	1	6	4
100,000	20,000	10,000	1	1	6	8
100,000	100,000	5000	1	4	19	5
250,000	50,000	10,000	1	3	12	7
100,000	100,000	5000	2	6	29	5
250,000	250,000	5000	1	10	40	4
250,000	250,000	5000	2	17	68	5

Score AI and Status AI service

Requirements for the device on which the Score AI and Status AI service is installed:

- CPU: 2.7 GHz or more, 2 cores.
- RAM: 8 GB.
- Storage: SSD or HDD.
- Free disk space: 10 GB for the service plus space for the operating system.

Software requirements

This section lists software requirements for the installation and operation of KUMA components and utilities.

Operating systems

The minimum compatible version of the Linux kernel on the target hosts is 5.15

The following operating systems are supported for installation of KUMA:

- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- Oracle Linux 8.10
- Oracle Linux 9.7
  More on upgrading from Oracle Linux 8.x to Oracle Linux 9.x.
- Red Hat Enterprise Linux 9.8
- Astra Linux Special Edition 1.7.7.9
- Astra Linux Special Edition 1.8.5
- Astra Linux Special Edition 1.8.6
- RED OS 7.3.4
- RED OS 8
- MosOS 15.6

Virtualization platforms

The following virtual environments are supported for installing KUMA:

- VMware 6.5 or later
- Hyper-V for Windows Server 2012 R2 or later
- QEMU-KVM 4.2 or later
- "Brest" virtualization software RDTSP.10001-02

- Nutanix 7.5.
- Basis Dynamix Enterprise 4.6

Working in cloud environments

KUMA can work in a cloud infrastructure. The solution can be installed on virtual machines following the IaaS (infrastructure-as-a-service) model.

For a cloud infrastructure, we recommend using the single-server configuration for 3000 EPS and 10,000 EPS. Virtual machines must satisfy the hardware and software requirements of a regular installation.

When choosing the disk subsystem of the server, use the number of input/output operations (IOPS) as the reference. The recommended minimum value is 1000 IOPS.

TLS ciphersuites

TLS versions 1.2 and 1.3 are supported. Integration with a server that does not support the TLS versions and ciphersuites that KUMA requires is impossible.

Supported TLS 1.2 ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Supported TLS 1.3 ciphersuites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Sigma rules converter

The converter is supported on the following operating systems:

- Ubuntu 2024
- Windows 10
- Windows 11
- RED OS 7
- RED OS 8
- Oracle Linux 8.3
- Oracle Linux 9.3
  More on upgrading from Oracle Linux 8.x to Oracle Linux 9.x.

The kuma-kont utility

The utility is supported on the following operating systems:

- Astra Linux
- Ubuntu 22.04 LTS
- RED OS 7.3.4
- RED OS 8

Requirements for Windows devices for agent installation

You must install agents on network infrastructure devices that will send data to the KUMA collector. The requirements for Windows devices for the installation and operation of KUMA agents are listed in this article.

System requirements

Minimum hardware requirements:

- CPU: 1.4 GHz or more, 1 core.
- RAM: 512 MB.
- Free disk space: 1 GB.

The following operating systems are supported:

- Microsoft® Windows® 2012 (limited support)
- Microsoft Windows 2012 R2 (limited support)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025
- Microsoft Windows 10
- Microsoft Windows 11

Hardware requirements for installing KUMA agents with WEC, ETW, and WMI connectors

KUMA agents installed on Windows devices can use various types of connectors to receive events: WEC (Windows Event Collector), ETW (Event Tracing for Windows), and WMI (Windows Management Instrumentation). The performance of the agents and their impact on the system depend on the limitations imposed by Windows and on the amount and type of events processed (see the table below).

Requirements for agents by connector type

Connector type	Maximum performance (EPS)	Limitations imposed by Windows	Limitations imposed by KUMA	Recommended agent configuration	CPU and RAM usage
WEC	Up to 2500 events per second	When writing to system logs (Application, System, Hardware Events), Windows limits the rate to approximately 2500 events per second. When writing to multiple logs at the same time, performance is further reduced: up to 1100 EPS with 2 logs, up to 800 EPS with 3 logs, and up to 500 EPS with 4 logs.	The agent can process events in the range of 1500–2500 EPS without lag.	CPU: 1 core with 2 threads or 2 vCPUs. RAM: 4 GB.	Average CPU load by the agent: up to 0.18 (equivalent to approximately 0.28% of the total system performance). RAM usage: up to 209 MB.
ETW	Up to 700 events per second	Only one system log is supported: **Microsoft → Windows → DNS-Server**. The Windows operating system does not allow writing more than 700 events per second to this log.	No limitations on the KUMA side have been identified, however, when EPS exceeds 700, the agent does not receive data due to Windows restrictions.	CPU: 1 core with 2 threads or 2 vCPUs. RAM: 4 GB.	Average CPU load by the agent: up to 0.267 (equivalent to approximately 0.42% of the total system performance). RAM usage: up to 186 MB.
WMI	Up to 5000 events per second	You can circumvent Windows restrictions by connecting multiple devices. Each additional device increases the total event volume that can be processed by 1000–1500 EPS.	Upon reaching 5000 EPS, the agent starts processing events with a lag.	CPU: 1 core with 2 threads or 2 vCPUs. RAM: 4 GB.	Average CPU load by the agent: up to 0.61 (equivalent to approximately 0.91% of the total system performance). RAM usage: up to 311 MB.

Requirements for Linux devices for agent installation

You must install agents on network infrastructure devices that will send data to the KUMA collector. The requirements for Linux devices for the installation and operation of KUMA agents are listed in this article.

System requirements

Minimum hardware requirements:

- CPU: 1.4 GHz or more, 1 core.
- RAM: 512 MB.
- Free disk space: 1 GB.

The following operating systems are supported:

- Oracle® Linux 8.x
- Oracle Linux 9.x
- Alma Linux 9.5
- Astra Linux Special Edition RUSB.10015-01 1.7.x (starting with version 2021-1126SE17, update 1.7.1) with glibc 2.28 (Debian GLIBC 2.28-10+deb10u4+ci202407161455+astra12).
- Astra Linux Special Edition RUSB.10015-01 1.8.x (starting with version 2025-0114SE18MD, update 1.8.1.UU.2) with glibc 2.36 (Debian GLIBC 2.36-9+deb12u7+ci202405171200+astra5).
- CentOS Linux release 8.2.2004 (Core) with glibc 2.28 (GNU libc).
- CentOS Linux release 7.7.1908 (Core) with glibc 2.17 (GNU libc).
- Debian 12 with glibc 2.36 (Debian GLIBC 2.36-9+deb12u7).
- Red Hat Enterprise Linux 9.5 (Plow) with glibc 2.34 (GNU libc).
- Red OS 8.
- Rocky Linux 9.3 (Blue Onyx) with glibc 2.34 (GNU libc)
- Rocky Linux 9.5.
- SuSE 15.6.
- Ubuntu 24.04.2 LTS with glibc 2.39 (Ubuntu GLIBC 2.39-0ubuntu8.4)

- Ubuntu 22.04.4 LTS with glibc 2.35 (Ubuntu GLIBC 2.35-0ubuntu3.8)
- MosOS 15.5

Device requirements depending on EPS

KUMA agents installed on devices running Linux use the HTTP transport type. The hardware requirements of KUMA agents depend on the event flow (EPS); see table below.

Hardware requirements of agents depending on EPS

	10,000 EPS	20,000 EPS	60,000 EPS	100,000 EPS
CPU	3 cores	5 cores	6 cores	6 cores
RAM	160 MB	160 MB	260 MB	300 MB

Requirements for devices running on Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS

Requirements for KUMA installation on devices running Oracle Linux, Astra Linux, Ubuntu, RED OS, and MosOS are provided in a table below.

	Oracle Linux	Astra Linux	Ubuntu	RED OS	MosOS
Python version	3.6 to 3.11. Hosts with Python earlier than 3.6 (inclusive) cannot be combined in the same instance with Python 3.10 and later hosts.	3.6 to 3.11. Hosts with Python earlier than 3.6 (inclusive) cannot be combined in the same instance with Python 3.10 and later hosts.	3.6 to 3.11. Hosts with Python earlier than 3.6 (inclusive) cannot be combined in the same instance with Python 3.10 and later hosts.	3.6 to 3.11. Hosts with Python earlier than 3.6 (inclusive) cannot be combined in the same instance with Python 3.10 and later hosts.	3.6 to 3.11. Hosts with Python earlier than 3.6 (inclusive) cannot be combined in the same instance with Python 3.10 and later hosts.
SELinux module	Disabled	Disabled	Disabled	Disabled	Disabled

	Oracle Linux	Astra Linux	Ubuntu	RED OS	MosOS
Package manager	pip3	pip3	pip3	pip3	pip3

Basic packages	• tar
	• systemctl
	• netaddr
	• firewalld
	More on upgrading from Oracle Linux 8.x to Oracle Linux 9.x.
	To install the packages, run the following commands:
	`pip3 install netaddr`
	`yum install firewalld`
		• tar
		• systemctl
		• python3-apt
		• curl
		• libcurl4
		To install the packages, run the following command:
		`apt install python3-apt curl libcurl4`
			• tar
			• systemctl
			• python3-apt
			• curl
			• libcurl4
			To install the packages, run the following command:
			`apt install python3-apt curl libcurl4`
				• tar
				• systemctl
				• netaddr
				• firewalld
				To install the packages, run the following commands:
				`pip3 install netaddr`
				`dnf install firewalld`
					• tar
					• systemctl
					• python3-rpm
					To install the package, run the following commands:
					`zypper refresh`
					`zypper install python3-rpm`

Dependent packages	No value	• netaddr • python3-cffi-backend To install the packages, run the following command: `apt install python3-netaddr python3-cffi-backend` If you plan to query Oracle DB databases from KUMA, you need to install the Astra Linux libaio1 package.	• netaddr • python3-cffi-backend To install the packages, run the following command: `apt install python3-netaddr python3-cffi-backend`	No value	No value

Packages that must be installed on a device with the KUMA Core for correct generation and downloading of reports	• nss
	• gtk2
	• atk
	• libnss3.so
	• libatk-1.0.so.0
	• libxkbcommon
	• libdrm
	• at-spi2-atk
	• mesa-libgbm
	• alsa-lib
	• cups-libs
	• libXcomposite
	• libXdamage
	• libXrandr
	To install the packages, run the following command:
	`yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`
		• libgtk2.0-0
		• libnss3
		• libatk-adaptor
		• libdrm-common
		• libgbm1
		• libxkbcommon0
		• libasound2
		To install the packages, run the following command:
		`apt install libgtk2.0-0 libnss3 libatk-adaptor libdrm-common libgbm1 libxkbcommon0 libasound2`
			• libatk1.0-0
			• libgtk2.0-0
			• libatk-bridge2.0-0
			• libcups2
			• libxcomposite-dev
			• libxdamage1
			• libxrandr2
			• libgbm-dev
			• libxkbcommon-x11-0
			• libpangocairo-1.0-0
			• libasound2 (for Ubuntu 22.04 LTS) or libasound2t64 (for Ubuntu 24.04 LTS)
			To install the packages, run the following commands:
			`For Ubuntu 22.04 LTS`
			`apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2`
			`For Ubuntu 24.04 LTS`
			`apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2t64`
				• nss
				• gtk2
				• atk
				• libnss3.so
				• libatk-1.0.so.0
				• libxkbcommon
				• libdrm
				• at-spi2-atk
				• mesa-libgbm
				• alsa-lib
				• cups-libs
				• libXcomposite
				• libXdamage
				• libXrandr
				To install the packages, run the following command:
				`dnf install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`
					No value

	Oracle Linux	Astra Linux	Ubuntu	RED OS	MosOS
User permissions required to install the solution	No value	High integrity level (63)	No value	No value.	No value

Packages to install on all target computers when deploying KUMA on a Kubernetes cluster	• iscsi-initiator-utils
	• wireguard-tools
	Before installing the packages on Oracle Linux, you must add the EPEL repository as a source of packages using one of the following commands:
	For Oracle Linux 8
	`sudo yum install oracle-epel-release-el8`
	For Oracle Linux 9
	`sudo yum install oracle-epel-release-el9`
	To install the packages, run the following command:
	`sudo yum install iscsi-initiator-utils wireguard-tools`
		• open-iscsi
		• wireguard
		• wireguard-tools
		To install the packages, run the following command:
		`sudo apt install open-iscsi wireguard wireguard-tools`
			• open-iscsi
			• wireguard
			• wireguard-tools
			To install the packages, run the following command:
			`sudo apt install open-iscsi wireguard wireguard-tools`
				• iscsi-initiator-utils
				To install the package, run the following command:
				`sudo apt install iscsi-initiator-utils`
				After installing the package, run the following commands:
				`sudo systemctl enable iscsid`
				`sudo systemctl start iscsid`
					No value

Requirements for client devices for managing the KUMA web interface

CPU:

- Intel® Core™ i3, 8th generation, 32-bit
- AMD Ryzen 3, 32-bit

RAM: 8 GB

Supported browsers:

- Google™ Chrome™ 131 or later
- Mozilla™ Firefox™ 115 or later

Device requirements for installing KUMA on Kubernetes

Minimum configuration of a Kubernetes cluster for deployment of a high-availability KUMA configuration:

- 1 load balancer node (the balancer is not part of the cluster)
- 3 controller nodes
- 2 worker nodes

The minimum hardware requirements for devices for installing KUMA on Kubernetes are listed in the table below.

Minimum hardware requirements for installing KUMA on Kubernetes

	Balancer	Controller	Worker node
CPU	1 core with 2 threads or 2 vCPUs.	1 core with 2 threads or 2 vCPUs.	12 threads or 12 vCPUs.
RAM	At least 2 GB	At least 2 GB	At least 24 GB
Free disk space	At least 30 GB	At least 30 GB	For new instances of KUMA: at least 600 GB of free disk space in the `/opt` directory. For existing KUMA instances: if 1 TB or more disk space has been previously allocated in the `/opt` directory, we do not recommend reducing disk space without expert advice from Technical Support. At least 50 GB in the `/var/lib` directory.
Network bandwidth	10 Gbps	10 Gbps	10 Gbps

Selecting hardware for ClickHouse cluster storages

When sizing the storage cluster, consider the EPS, the average event size and the retention period, as well as the requirements for the disk subsystem, network interface, RAM, and usage profile.

Disk subsystem

Write (insert) operations constitute the majority of the load that KUMA places on ClickHouse:

- Events arrive in the database in an almost constant stream.
- Inserts are small and frequent by ClickHouse standards.
- ClickHouse has high write amplification because of the constant merging of partition parts in the background.
- A partition part under 1 GB in size is stored as one file. When a part reaches 1 GB, wide column format is applied, wherein each column of the table is represented by two files, .dat and .mrk. In this case, overwriting a partition part to merge it with another part requires writing to 384 files + fsync for each, which is a lot of IOPS.

ClickHouse handles search queries at the same time, but there are much fewer of those than write operations. Considering the load profile, we recommend organizing the disk subsystem in the following way:

- Use DAS (Direct Attached Storage) with NVME or SAS/SATA interfaces, avoiding SAN/NAS solutions.
- If the nodes of the ClickHouse cluster are deployed in a virtual environment, the disk array must be directly mounted to the `/opt/kaspersky/kuma` directory. Avoid virtual disks.
- Use SSD (SATA/NVME). Any server-grade SSDs will outperform HDDs (even 15,000 RPM). For SSDs, use RAID-10 or RAID-0 (if replication is used in ClickHouse).

  If SSDs cannot be used, use 15,000-RPM SAS HDDs in RAID-10.

  A hybrid option is possible: storing hot data (for example, for the last month) on SSDs, and cold data on HDDs. This arrangement makes sure the SSD arrays always handle the write operations.

When using hybrid storage with SSDs and HDDs, keep in mind that a software RAID array (madm) will always outperform a hardware RAID controller and offer more flexibility. When using RAID-0 or RAID-10, it is important that the stripe size be 1 MB. In hardware RAID controllers, the default stripe size is often 64 KB, and the maximum supported value is 256–512 KB. For RAID-10, near-layout is optimal for writing, and far-layout is optimal for reading.

- We recommend EXT4 as the file system. If EXT4 cannot be used, XFS is acceptable. We recommend enabling the 'noatime' mount option for either of these file systems.

Network interface

Recommendations for the network interface:

1. On each node of the cluster, a network interface with a bandwidth of at least 10 Gbps must be installed with appropriate switching. Considering write amplification and replication, 25 Gbps is ideal.

2. If necessary, replication processes can use a separate network interface that does not handle insert and search traffic.

RAM

ClickHouse recommends a ratio of the RAM size to data stored on a node of 1:100.

However, when sizing the RAM, you need to consider not just the total amount of stored data, but also how much data is processed on average when running queries. For example, if the average query involves scanning partitions with a total volume of 10 TB, at least 100 GB of RAM is recommended. This ratio is a general recommendation and is tailored to broad analytical queries. Actual memory requirements depend on the nature of the queries, the amount of data being processed, and the configuration of the system.

Having free memory on the server improves the performance of search queries for the most recent events because the contents of the partition files are duplicated in the operating system's cache, allowing it to be read from RAM, not the disk.

Usage profile

The hardware requirements are designed for the database to ingest a stream of a certain EPS when the database is at rest (no search queries are being executed, only write operations). At the KUMA deployment stage, it is not always possible to accurately determine what kind of search and analytical queries the system will process, the intensiveness, concurrency, and depth of search queries, as well as the actual performance of the cluster nodes.

Thus, scaling a ClickHouse cluster during the operation of KUMA is a commonplace scenario. If an increase of EPS or intensity or resource consumption of search queries makes the cluster unable to cope with the load, you can add more shards (horizontal scaling) or improve the disk subsystems, CPU, or RAM on the cluster nodes.

EPS-dependent hardware configurations and scaling

The table below describes the configurations and recommended resources for KUMA components depending on the EPS level, including storage requirements and sizing recommendations.

Recommended hardware configurations and resource consumption by KUMA depending on EPS

Setting	Up to 3,000 EPS	Up to 10,000 EPS	Up to 20,000 EPS	Up to 50,000 EPS
Installation type	Installation on a single server	Installation on a single server	Distributed installation on multiple servers	Distributed installation on multiple servers
Number of servers and their purpose	1 server that hosts all system components.	1 server that hosts all system components.	1 server for the KUMA Core. 1 server for the collector. 1 server for the correlator. 3 dedicated servers with the keeper role. 2 servers for the storage.	1 server for the KUMA Core. 2 servers for the collector. 1 server for the correlator. 3 dedicated servers with the keeper role. 4 servers for the storage.
Server hardware	See the hardware requirements.	See the hardware requirements.	See the hardware requirements. The storage requires fast SSDs, high IOPS, at least 1 Gbps of network bandwidth.	Same specifications as for EPS 20,000, but with twice the number of collectors and storage servers. Higher requirements for network connectivity between all nodes: at least 1 Gbps of network bandwidth is recommended.
Storage configuration (ClickHouse)	1 shard, 1 replica. Disk buffer enabled.	1 shard, 1 replica. Disk buffer enabled.	2 shards, 2 replicas in each. If high availability is not required, 1 server with 1 replica per shard may be used.	2 shards, 2 replicas in each. If high availability is not required, 2 servers with 1 replica per shard may be used.

Additional recommendations for specifying and sizing the configuration:

- For the KUMA Core, if you have more than 50,000 assets, we recommend increasing the resource allocation. For every additional 50,000 assets, you need to add 2 threads (or 2 vCPUs) and 4 GB of RAM.

  If the system manages more than 100 services, you need to account for the additional load. For every 100 services, you also need to increase the computational resources of the KUMA Core by 2 threads (or 2 vCPUs).

- If users actively engage with the system, including frequent generation of reports, using dashboards, and running custom SQL queries, you need to adjust the sizing of both the KUMA Core and the storage because such activity substantially increases the load on both components.

- When choosing the disk subsystem for the storage (ClickHouse), only SSD drives may be used. An exception is possible if you do not plan to run aggregation SQL queries with a depth of more than 24 hours. In this case, you may use HDDs with the following minimum specifications: 15,000 RPM, SAS interface, RAID-10.

- When placing components in HDFS, you may use HDD regardless of the queries that you run.

- Events are exported via temporary files that are saved in the `/opt/kaspersky/kuma/core/tmp` directory. These files are automatically deleted after 10 days. If you plan to export a large amount of events, you must allocate additional space.

Distribution kit

The distribution kit includes the following files:

- `kuma-ansible-installer-<build number>.tar.gz`, used to install KUMA without using Kubernetes. You can perform a distributed installation with the KUMA Core in a Raft-based cluster.
- `kuma-ansible-installer-k8s-<build number>.tar.gz`, used for installing KUMA in a high-availability configuration based on Kubernetes.
- Files containing information about the version (release notes) in Russian and English

For the certified version of KUMA, the installer is delivered as two archives:

- `kuma-ansible-installer-<build number>-certified.tar.gz`, containing the certified part of the distribution kit to which the certificate applies.
- `kuma-ansible-installer-<build number>-environment.tar.gz`, containing components that are included in the certified distribution, but are not subject to certification (for example, installers of third-party components and other auxiliary code).

These archives form parts of one overall distribution kit. Before installation, you need to extract the contents of both archives into the same `kuma-ansible-installer` directory. For example, for version 4.0.2.13, the contents of the `kuma-ansible-installer-4.0.2.13-certified.tar.gz` and `kuma-ansible-installer-4.0.2.13-environment.tar.gz` archives must be extracted into the same `kuma-ansible-installer` directory to combine their contents. After combining the contents in this way, the installation proceeds as usual.

Each archive contains a set of files required for working with KUMA.

A set of files for working with KUMA

File name	Description
Scripts	
`install.sh`	Script for installing and upgrading KUMA.
`postinstall.sh`	Script for preparing hosts for installing services. Used when activating with an activation code.
`expand.sh`	Script for adding hosts and services to an existing configuration.
`change_url.sh`	Script for changing the hostname and reconnecting services to the KUMA Core.
`uninstall.sh`	Script for uninstalling KUMA.
`cluster_upgrade.sh`	Script for upgrading a Kubernetes cluster.
Inventory file templates	
`single.inventory.yml.template`	Inventory file template for deployment in an all-in-one configuration.
`distributed.inventory.yml.template`	Inventory file template for deployment in a distributed configuration with a single KUMA Core or with multiple Core services combined into a Raft cluster.
`k0s.inventory.yml.template`	Inventory file template for deployment in a Kubernetes cluster.
`expand.inventory.yml.template`	Inventory file template for adding hosts to an existing configuration for the subsequent installation of services on these hosts.
Utilities and agents	
`kuma.exe`	KUMA agent for Windows installation file.

File name	Description
`agent.exe`	KUMA agent for Linux installation file.
`kuma-sigma-converter-0.1.0.tar.gz`	Archive with Sigma converter installation files.
`kuma-ptvm.tar.gz`	Archive with the tool for importing data from MaxPatrol VM.
`max-patrol-tool`	Tool for importing data from MaxPatrol 8.
`kuma-kont.tar.gz`	Archive with the tool for importing data from the database of the Continent 3.9.2 system.
`integrity.tar.gz`	Archive with scripts for checking the integrity of the solution.
Legal information	
`license`	The End User License Agreement.
`legal_notices`	Legal notices.

Architecture of the solution

The standard solution installation includes the following components:

- The *Core* is the central component of KUMA that serves as a foundation for all other services and components deployment. The Core provides a graphical web interface for configuring and managing system components, visualizing data, and conducting investigations.

  The Core allows you to:

  - Create and configure services (or components) of the solution, as well as integrate the necessary software into the system.
  - Manage services and user accounts of the solution in a centralized way.
  - Visualize solution performance statistics.
  - Investigate security threats based on the received events.

- One or more collectors. A *Collector* receives events from different sources and brings them to a unified data schema, allowing you to aggregate events by a certain criterion or to enrich events with additional information. The collector sends events to the storage, correlator and/or third-party services to detect alerts.

- The *correlator* analyzes incoming events and detects alerts according to the logic defined in the correlation rules. Active lists, context tables, and local variables can be used to extend the correlation context.

- A *storage* is a service that acts as an intermediary between the ClickHouse cluster and other KUMA services. The storage service collects data from collectors and correlators and transfers it to the ClickHouse cluster. The storage service manages the ClickHouse cluster and the storage settings for the collected data. Built-in ClickHouse cluster functionality provides database clustering, data transfer between hot and cold storage, and data archiving.

- *Metrics* is a component of the solution that provides collection, storage, and visualization of operating parameters of KUMA components.

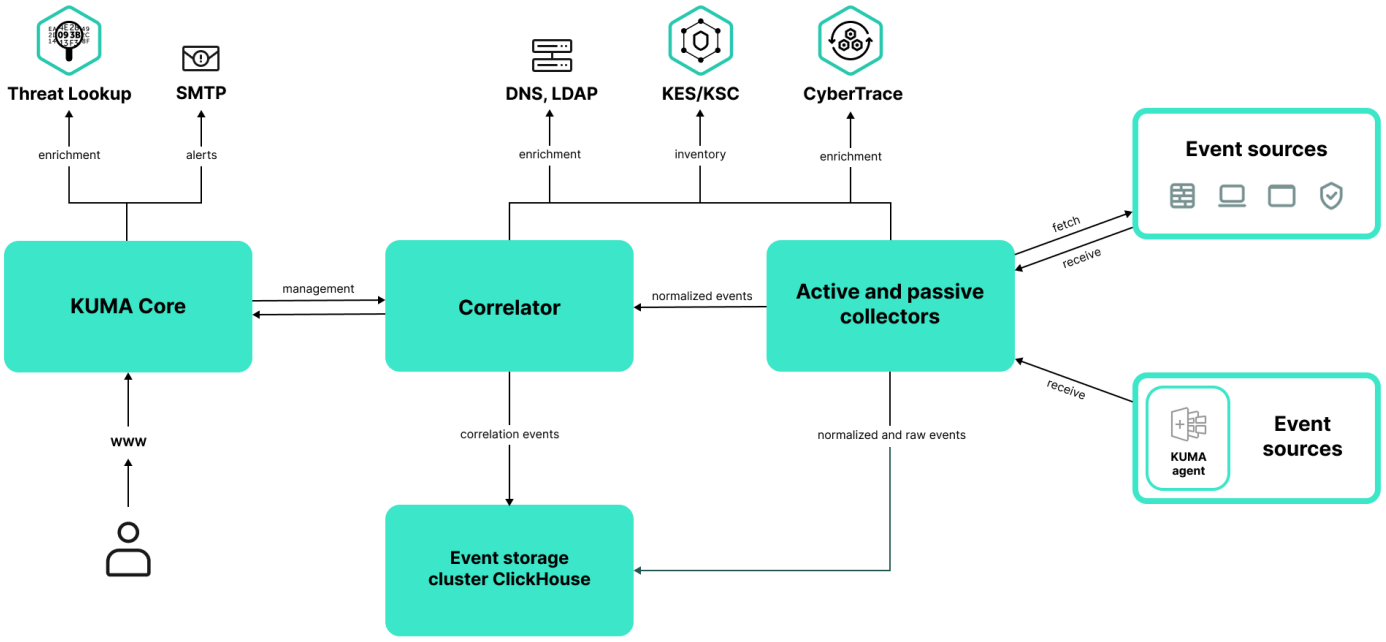
- *Event routers* that receive events from collectors and apply the configured filters to route the events to the configured destinations.

  The event router service is optional. It may be required in companies with branches, when there are narrow or overloaded communication channels between the data center with correlators, event storages, and a remote branch. In this case, an event router can be installed in the data center, and collectors in the remote branch can be configured to send data to the router instead of sending it separately to correlators and storage. This reduces the load on network channels.

- *Agents* send raw events from Windows and Linux servers and workstations to KUMA destinations.

  If necessary, an agent can be used to balance the stream of events among multiple KUMA components and to automatically switch to a standby component if the primary component becomes unavailable.

All KUMA services send events between components using robust transport protocols with encryption support. If a destination is unavailable, the service saves events in a local file system buffer and transmits them after the connection is restored. The size of the buffer for temporary storage of events is configurable.



KUMA architecture

Deployment and initial configuration

Following this scenario, you can deploy Kaspersky SIEM with all components required for the solution and perform the initial configuration. For each stage, there are links to instructions for performing the necessary steps and additional materials for review.

1 Choosing a deployment configuration

Before deploying Kaspersky SIEM, select the deployment configuration that best suits your infrastructure. The following articles may be helpful for making a decision:

- descriptions and diagrams of the available deployment configurations, and a comparison table with key selection criteria;
- system scalability requirements.

If infrastructure requirements change in the future, the deployment configuration can be changed.

2 Installation preparation

After choosing the appropriate configuration, complete the preparatory steps on all computers where the solution will be deployed.

3 Installing the solution

Once the infrastructure is prepared, proceed with installation according to the selected deployment configuration:

- Installation on a single server;
- Installation in a distributed configuration;
- Installing in a high availability configuration in a Kubernetes cluster;
- Installing in a high availability configuration in a Raft cluster.

4 Post-installation steps

After installation is complete, do the following:

- Change the administrator password.
- If necessary, replace the self-signed certificate with a corporate one.

After completing these steps, you can proceed to the initial configuration.

5 Initial configuration

After successful deployment, you need to perform the initial Kaspersky SIEM configuration to prepare the system for full operation:

- Integration with Active Directory and adding users, assigning roles

  Configure the integration with Active Directory to enable authentication using a domain account or create users manually. Then assign roles to all users.

- Multi-tenant configuration

  If necessary, configure the tenant structure to manage user access and determine the interaction between KUMA resources and services.

- Configuring event sources, storage, and correlation

  Specify where events are received from and how they should be stored and processed:

  - Configure integration with Kaspersky Security Center.
  - Import assets from Kaspersky Security Center.
  - Add assets manually or import them from other sources (optional).
  - Configure event sources to specify where to receive events from.
  - Create storage for events.
  - Create collectors to receive, process (normalize), and transfer events.
  - Create correlators for the initial analysis of normalized events and their further processing.

  When creating a correlator, you can add correlation rules that define rules for processing and responding to events, import correlation rules that were previously saved or presented in the repository, or use a ready-made set of correlation rules included in the Kaspersky SIEM distribution kit. After creating the correlator, you can link correlation rules with the correlator.

  > It is recommended to configure exclusions at this stage to avoid false positives and irrelevant data.

- Configuring notifications

  Configure the connection to the SMTP server to receive email notifications.

- Configuring integrations

  Configure the integration with Kaspersky solutions to expand the capabilities and enrich the data available for incident investigation.

- Checking the correctness of the initial configuration

  If the initial configuration is performed correctly, the services are displayed in a green status. After restarting the service, an audit event appears in the **Events** section. If the event sources are configured correctly, the event search returns the corresponding records.

After the initial configuration is complete, Kaspersky SIEM will receive and process events from protected assets, and an alert will be generated when a correlation rule is triggered.

Choosing a deployment configuration

These instructions are part of the deployment and initial configuration scenario.

KUMA's microservice architecture enables flexible deployment configuration. Choosing the right deployment type for your infrastructure depends on many aspects, such as event stream, data availability requirements, available hardware resources, and scalability considerations.

This article provides descriptions and graphical diagrams for four supported deployment configurations. The diagrams illustrate possible infrastructure configurations and can be adapted to the requirements of your organization.

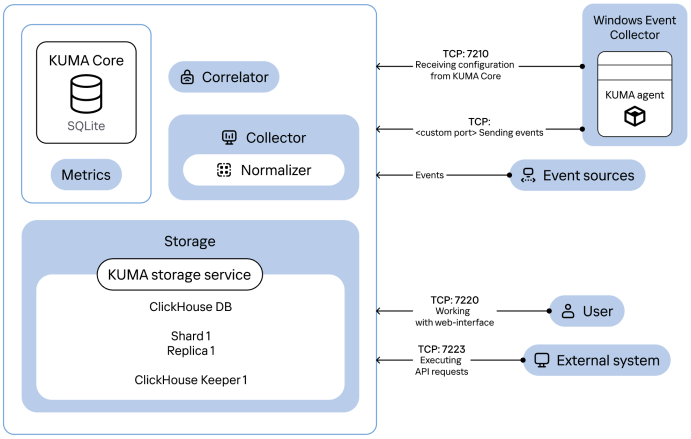
Deployment on a single server

The KUMA Core and all solution services are installed on the same server and interact locally.

This type of deployment is suitable for pilot projects or small-scale infrastructure with a limited event stream (up to 10,000 EPS).

The diagram below shows the placement of KUMA components in a single-server deployment.

Single-server deployment diagram



Installation on a single server

Advantages:

- Easy to install and maintain.
- Minimum infrastructure requirements.
- Ability to switch to a distributed deployment scheme in the future without reinstalling the system.

Limitations:

- Lack of fault tolerance. If the server fails, all KUMA services become unavailable.
- Limited scalability. If the load exceeds the recommended level, performance may decrease. If necessary, you can change the configuration to distributed to balance the load.

Distributed deployment

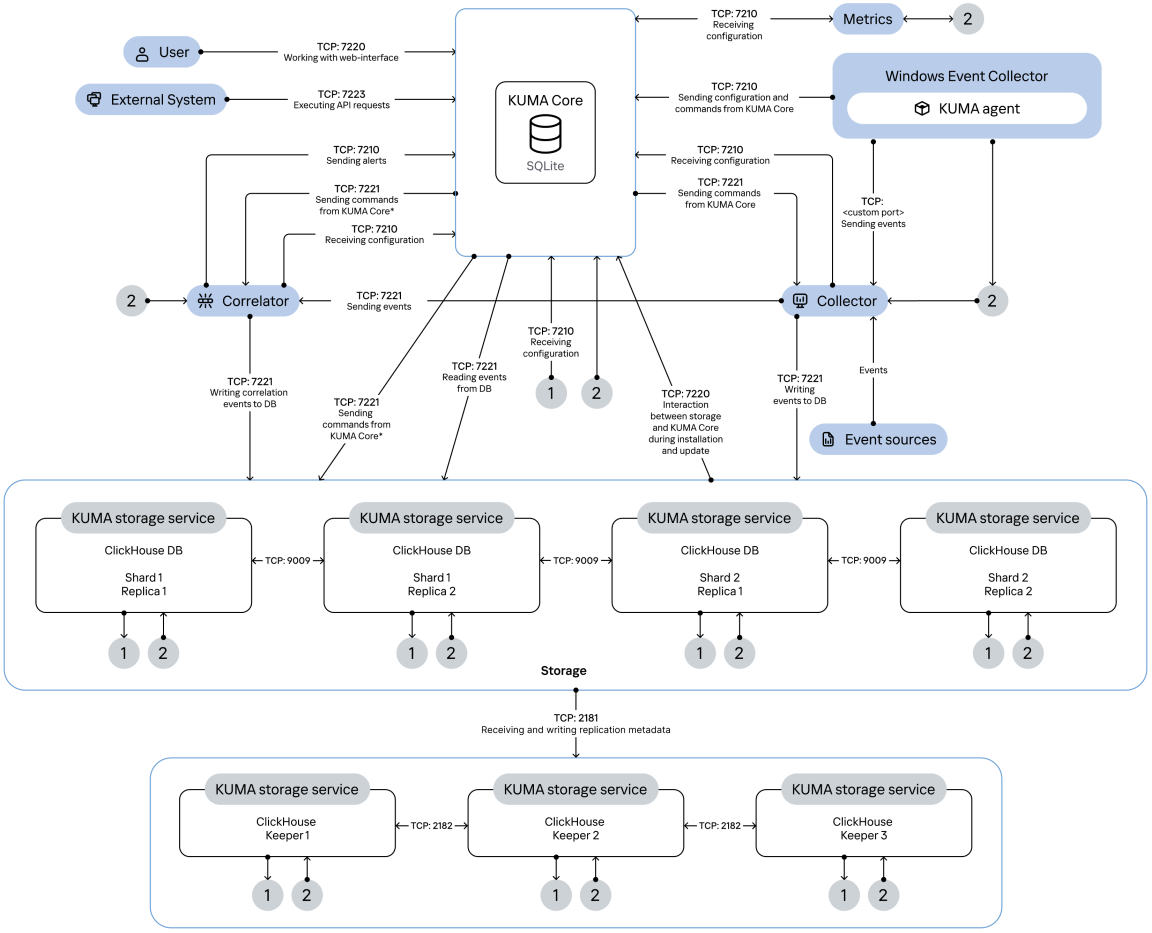
KUMA Core is installed on a separate server, while services are hosted on different servers and interact with KUMA Core over the network. It is possible to install multiple services on a single server. For example, you can install the KUMA Core and collector on the same server, and the storage and correlator on separate servers. This type of configuration also allows you to create duplicate collector, correlator, and storage services, where data is divided into shards with one or more replicas (two replicas are recommended).

This type of deployment is suitable not only for high-load infrastructure (over 10,000 EPS), but also for small geo-distributed infrastructures, for example:

- The branch is located in Chukotka and uses satellite-based internet. The branch office installs a collector, correlator, and storage, while management and analytics are performed at the head office.
- Distributed event storage across two data centers: even-numbered nodes are in data center A, and odd-numbered nodes are in data center B. If one data center fails, the data remains available.

The diagram below shows the placement of KUMA components in a distributed deployment.

Distributed deployment scheme



Distributed Installation diagram

Advantages:

- Improved performance through load balancing across servers.
- More flexible resource configuration for different components.
- The possibility of horizontal scaling (adding servers) and vertical scaling (adding CPU, memory, and disk space) on a running server without affecting the entire solution.

Limitations:

- Lack of fault tolerance of the KUMA Core service. If KUMA Core fails, services continue to operate as before (event collection, correlation, and storage), but since KUMA Core is unavailable, it is not possible to change service settings or restart services.
- It is required to ensure network connectivity between servers and consistency of DNS and NTP settings.

Deployment in a Kubernetes cluster

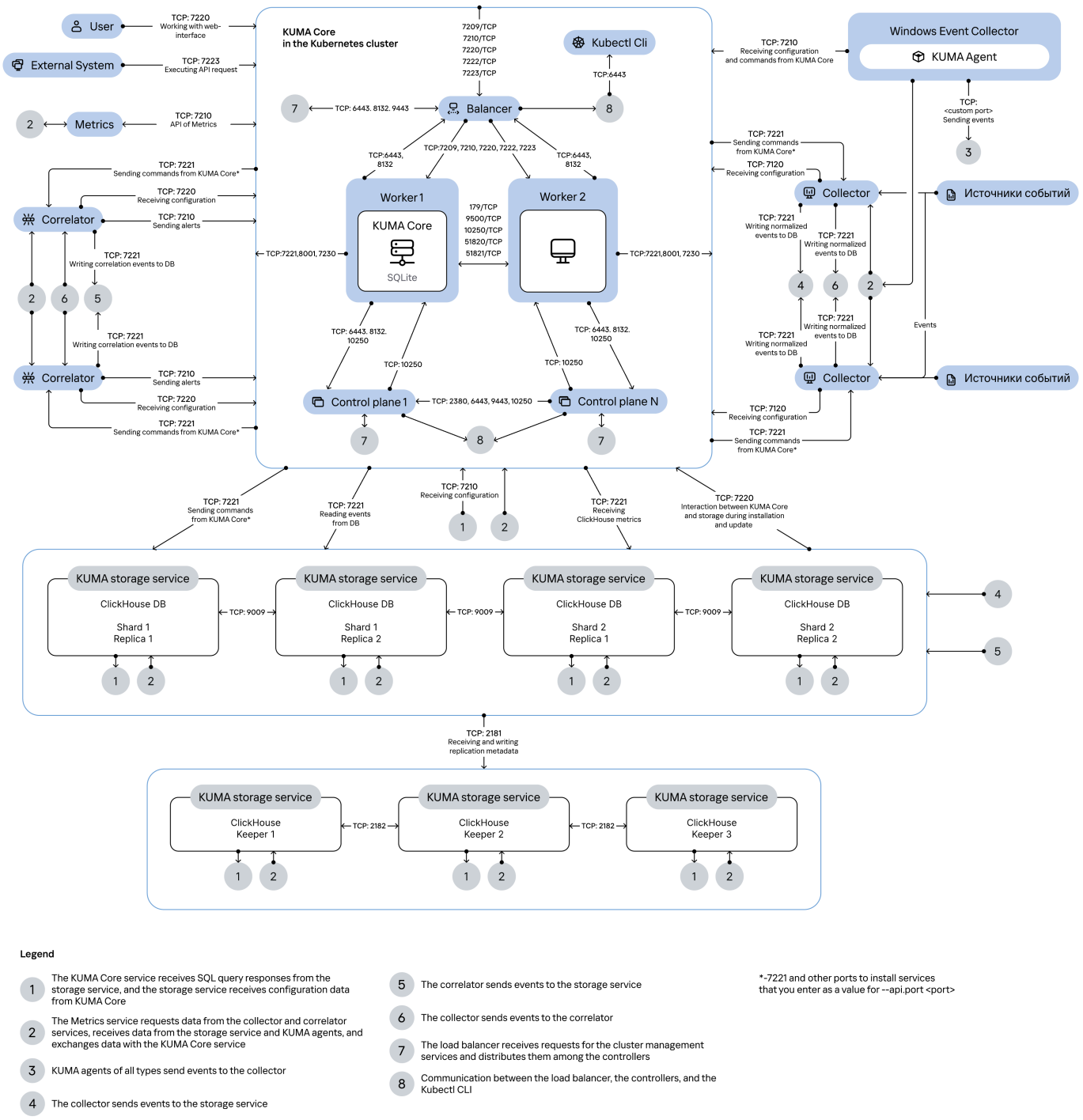
KUMA Core is installed in a high-availability Kubernetes cluster, while other services are installed on separate servers.

This type of deployment is suitable for dynamic infrastructure where high availability and scalability are important, for example:

- A cloud environment with a large number of nodes and dashboards, where services can automatically scale.
- Suitable for teams with experience of operating Kubernetes who want to update components without stopping the system.

The diagram below shows the placement of KUMA components in a Kubernetes cluster deployment. KUMA Core services run on worker nodes in the Kubernetes cluster, while KUMA services are installed outside the cluster. The balancer distributes the load and ensures that services interact with the active KUMA Core instance over the network.

Deployment scheme in a Kubernetes cluster



Legend

1. The KUMA Core service receives SQL query responses from the storage service, and the storage service receives configuration data from KUMA Core
2. The Metrics service requests data from the collector and correlator services, receives data from the storage service and KUMA agents, and exchanges data with the KUMA Core service
3. KUMA agents of all types send events to the collector
4. The collector sends events to the storage service
5. The correlator sends events to the storage service
6. The collector sends events to the correlator
7. The load balancer receives requests for the cluster management services and distributes them among the controllers
8. Communication between the load balancer, the controllers, and the Kubectl CLI

*-7221 and other ports to install services that you enter as a value for --api.port <port>

Distributed installation in a high-availability configuration (Kubernetes cluster)

Advantages:

- High data availability.
- Ability to update components without stopping the system.

Limitations:

- A prepared Kubernetes infrastructure is required.
- More complex configuration and monitoring of the solution state.
- Lack of horizontal scaling of the KUMA Core service.
- When the KUMA Core service is moved between worker nodes, short-term downtime (several minutes) may occur.
- Increased requirements for hardware resources.
- Not suitable for certified deployments.

If a certified configuration with a fault-tolerant KUMA Core is required, as well as distribution of KUMA Core servers across multiple data centers, it is recommended to use the KUMA Core Raft cluster deployment scheme.

For more information, see Interaction of nodes in a Kubernetes cluster.

Deployment in a Raft cluster

KUMA Core is installed in a high availability Raft cluster, while other services are installed on separate servers. KUMA Core is deployed in multiple instances on separate servers and unified into a Raft cluster to ensure fault tolerance, while solution services are hosted on separate servers and interact with the KUMA Core cluster.

To ensure correct cluster operation, the number of KUMA Core nodes must be odd: three, five, or seven. A load balancer (not included in the distribution kit) allows requests to be distributed across KUMA Core services and is used, for example, when configuring domain authentication through AD FS so that users do not need to authenticate separately on each cluster node.

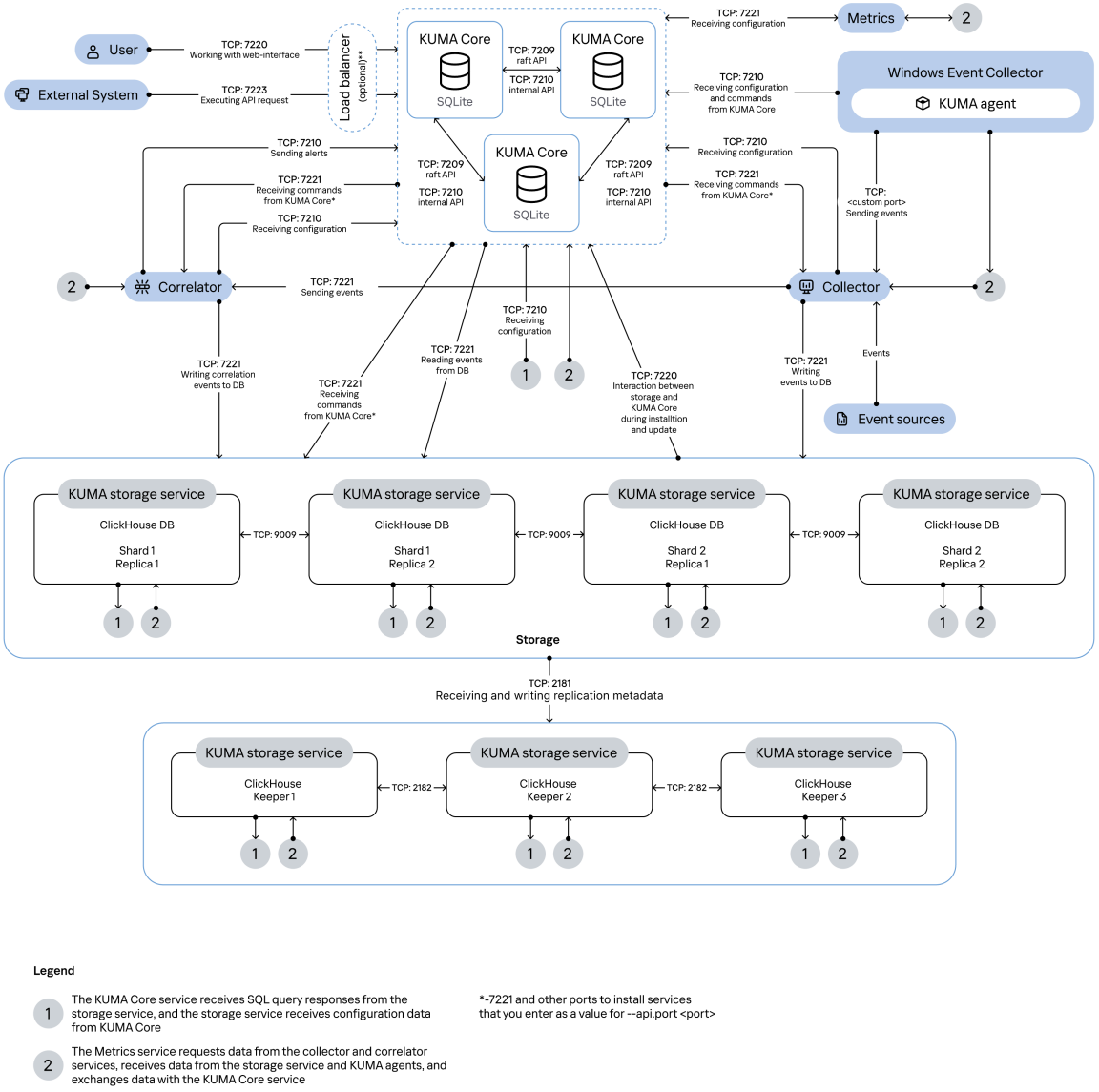
If necessary, KUMA services can be configured to access any available KUMA Core service.

This type of deployment is suitable for infrastructure without containerization, where KUMA Core fault tolerance and system stability are important, for example:

- An enterprise with several servers in the same data center, where KUMA Core scaling is rarely required or is performed manually.
- Suitable for a team with no experience of operating Kubernetes, where it is important that the cluster continues to function when individual nodes fail.

The diagram below shows the placement of KUMA components in a Raft cluster deployment.

Deployment scheme in a Raft cluster



Distributed installation in a high-availability configuration (Raft cluster)

Advantages:

- Provides fault tolerance. Failure of one or more KUMA Cores does not affect the availability of the solution, provided that most cluster servers remain available (for example, two out of three or three out of five servers).
- Ability to deploy geo-distributed infrastructure if RTT (round-trip time) between KUMA Core servers is less than 200 ms.
- Horizontal scaling for read operations.
- If necessary, a certified configuration of the KUMA Core with fault tolerance is provided.
- No downtime when switching between KUMA Core services.
- Data consistency is ensured by the Raft algorithm.

- Suitable for mission-critical services requiring continuous operation.
- Simpler architecture compared to Kubernetes.

Limitations:

- Requires more hardware resources than a single KUMA Core installation.

For more details, see the Interaction of Kaspersky SIEM components with a Raft cluster section.

Comparing deployment configurations

The table below provides a comparison of deployment types based on common criteria.

Comparison of deployment types by key characteristics

	Deployment on a single server	Distributed deployment	Deployment in a Kubernetes cluster	Deployment in a Raft cluster
KUMA Core fault tolerance	—	—	✓	✓
Scalability	Vertically	Vertically and horizontally	Vertically and horizontally	Vertically and horizontally
Hardware resources	Minimum	Medium	Maximum	Maximum
Certification	✓	✓	—	✓
Installation on physical or virtual servers without containerization	✓	✓	—	✓
Ease of operation	✓	Depends on configuration	—	Depends on configuration
Requires experience with Kubernetes	—	—	✓	—

Interaction of nodes in a Kubernetes cluster

Deploying KUMA Core in a Kubernetes cluster with an external TCP load balancer provides a fault-tolerant solution.

There are two possible roles for nodes in Kubernetes:

- Controllers (control-plane): nodes with this role manage the cluster, store metadata, and distribute the workload.
- Work nodes (worker): nodes with this role bear the workload by hosting Kaspersky SIEM processes.

Minimum configuration

To deploy Kaspersky SIEM in a high availability configuration, you need:

- 3 dedicated controllers
- 2 worker nodes
- 1 TCP balancer

To ensure the adequate performance of the KUMA Core in Kubernetes, you must allocate 3 dedicated nodes that have only the controller role. This provides high availability for the Kubernetes cluster and ensures that the workload (KUMA processes and other processes) cannot affect the tasks associated with managing the Kubernetes cluster. If you are using virtualization tools, make sure that the nodes are hosted on different physical servers and that these physical servers are not being used as worker nodes.

For a demo installation of KUMA, you may combine the controller and worker roles. However, if you are expanding an installation to a distributed installation, you must reinstall the entire Kubernetes cluster and allocate 3 dedicated nodes with the controller role and at least 2 nodes with the worker role. If there are nodes that combine the roles of a controller and a worker node, the upgrade of Kaspersky SIEM to the next version is not available.

Time zone in a Kubernetes cluster

The time zone within a Kubernetes cluster is always UTC+0, so this time difference should be taken into account when handling data created by the KUMA Core deployed in a high availability configuration:

- In audit events, the time zone in the `DeviceTimeZone` field is UTC+0.
- In generated reports, the difference between the report generation time and the browser' time will be displayed.
- In the dashboard you will find the difference between the time in the widget (the time of the user's browser is displayed) and the time in the exported widget data in the CSV file (the time of the Kubernetes cluster is displayed).

KUMA performance under various failure scenarios

Malfunction or network disconnection of the worker node where the KUMA Core service is deployed.

Access to the Kaspersky SIEM web interface is lost. After 6 minutes, Kubernetes initiates migration of the Core bucket to an operational node of the cluster. After the deployment, which takes less than one minute, is completed, the KUMA web interface becomes available again at URLs based on the FQDN of the load balancer. To determine on which of the hosts the Core is running, run the following command in the terminal of one of the controllers:

```
k0s kubectl get pod -n kuma -o wide
```

When the malfunctioning worker node or access to it is restored, the KUMA Core bucket is not migrated from its current worker node. A restored node can participate in replication of a disk volume of the KUMA Core service.

A worker node that contains a replica of the KUMA Core disk, and which is not hosting the KUMA Core service at the moment, fails or loses network connectivity.

Access to the Kaspersky SIEM web interface is possible via URLs that use the FQDN of the load balancer. The network storage creates a replica of the running KUMA Core disk volume on other running nodes. There is also no disruption of access to Kaspersky SIEM at URLs based on the FQDNs of currently operational nodes.

Loss of availability of one or more cluster controllers when quorum is maintained.

Worker nodes work normally. Access to Kaspersky SIEM is not disrupted. A failure of cluster controllers extensive enough to break quorum leads to the loss of control over the cluster.

Correspondence of the number of computers in use to ensure high availability

Number of controllers when installing a cluster	Minimum number of controllers required for the operation of the cluster (quorum)	Admissible number of failed controllers
1	1	0
2	2	0
3	2	1
4	3	1
5	3	2
6	4	2
7	4	3
8	5	3
9	5	4

Simultaneous failure of all Kubernetes cluster controllers.

The cluster cannot be managed and therefore will have impaired performance.

Simultaneous loss of availability of all worker nodes of a cluster with replicas of the KUMA Core volume and the KUMA Core pod.

Access to the Kaspersky SIEM web interface is lost. If all replicas are lost, information will be lost.

Interaction of Kaspersky SIEM components with a Raft cluster

Kaspersky SIEM supports a fault-tolerant cluster configuration based on the Raft consensus algorithm. The Raft cluster includes only KUMA Core services. The rest of the platform components (collectors, correlators, storages, routers, agents) operate outside the cluster and interact with the KUMA Core as external services.

The operation of KUMA Cores that are united in a Raft cluster provides the following:

- consistent storage of service configuration;
- synchronization of state among instances of the KUMA Core;

- high availability of data;
- automatic selection of the leading node.

For correct operation, at least three instances of KUMA Core and an odd number of nodes are required to ensure a quorum (see table below).

Allowed number of failed nodes depending on the number of nodes in the Raft cluster

Number of nodes in the Raft cluster	Allowed number of failed nodes
3	1
5	2
7	3

Interaction of KUMA Core services within the cluster

All instances of the KUMA Core interact directly with each other.

At each moment of time, one of the nodes acts as a Leader, and the rest work as Followers.

Leader is responsible for the following tasks:

- handling configuration changes;
- replication of changes to other KUMA Core services;
- coordination of the cluster state;
- receiving requests for write operations and broadcasting to other cluster nodes.

Followers do the following:

- receive updates from the leader;
- confirm replication;
- participate in the election of a new leader in case of failure of the current one;
- execute user requests to read data from the local SQLite database.

All services of the KUMA Core must have direct network accessibility to each other.

Interaction of components within the cluster includes:

- exchange of heartbeat messages;
- election of a leader in case of failure of the existing node;
- replication of the Raft log;
- synchronization of the configuration of KUMA services;
- transferring the service state of KUMA services.

Interaction of external services with the KUMA Core without a balancer

Without an external balancer, the solution services connect directly to the KUMA Core services.

In this case, the following conditions must be met:

- Each service must know the addresses of KUMA Cores.
- The list of KUMA Core URLs was specified when installing or configuring an external service.
- Addresses are passed either as a comma-separated list or by the multiple specifying of the `--core <url>` parameter.

  Example of a storage installation command:

  ```
  sudo /opt/kaspersky/kuma/kuma <storage> --core
  https://core1.example.com:7210,https://core2.example.com:7210,https://core3.example.com:7210 --pair.fingerprint
  <CA_cert_ID> --id <service_ID> --install
  ```

  where:

  - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

    The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
    You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

    To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

  - <service_ID> is the service ID copied from the KUMA web interface.

As a result, all platform components receive a list of KUMA Core instances and connect to one of the available Raft cluster nodes. If the current KUMA Core becomes unavailable, they switch to another URL from the list.

At the same time, external services do not participate in the internal interaction of the Raft cluster.

Features of operation without a balancer

Advantages:

- There is no additional infrastructure component.
- The deployment scheme is simplified.
- The number of intermediate points of failure is reduced.

Limitations:

- It is required to keep a list of all KUMA Cores in the configuration of each service.
- When changing the cluster composition, you need to update the configuration of external services.
- There is no single entry point to the web interface.
- If the current KUMA Core instance becomes unavailable, the external service sequentially attempts to establish a connection with other KUMA Cores specified in the configuration.

Interaction of KUMA Core services through the balancer

An external balancer can be used as a single entry point for access to the KUMA Core services. At the same time, the interaction among the services of the KUMA Core within the Raft cluster remains direct and does not pass through the balancer.

The balancer is not included in the KUMA distribution kit and deployed separately using the customer's infrastructure.

Interaction of external services with KUMA Cores through the balancer

If you have a configured balancer, you can use SSO (Single Sign-On). Since all user requests go through a single entry point, the balancer becomes the integration point for centralized authentication mechanisms.

External KUMA services interact with the Raft cluster through the balancer as follows:

- External services send requests to the balancer address and work with only one URL, for example, `https://kuma-load-balancer.example.com`.
- The balancer distributes requests among the KUMA Core services.
- If a Raft cluster node fails, routing automatically switches to another instance of the KUMA Core.

At the same time, the interaction among the services of the KUMA Core within the Raft cluster remains direct and does not pass through the balancer.

Installation preparation

These instructions are part of the deployment and initial configuration scenario.

Before installing KUMA, you have to prepare the infrastructure and configure access among the computers.

The preparation involves two steps:

1. **Infrastructure preparation**: configuring the reference and target computers, including system settings, network, and time synchronization.

2. **Generating SSH keys and configuring access**: ensuring connectivity from the control computer to the target computer via SSH to complete the installation.

The following are instructions for each step:

Preparing the infrastructure

KUMA is deployed centrally and involves a clear division of roles between the control and target computers.

The *control computer is* the host from which the installation is performed. The Ansible installer is started on the control computer, which connects to other servers via SSH and manages component deployment.

Target computers are servers on which KUMA components are installed (KUMA Core, collectors, correlators, storage, and other services).

The control computer can also act as a target if KUMA components are deployed on it. In this case, all requirements for the target computers apply to it. When deploying KUMA in a Kubernetes cluster, do not use the balancer node as a control computer to run the KUMA installer.

If the control computer is dedicated (for example, the administrator's laptop) and does not participate in installing KUMA components, only time synchronization needs to be configured on it (see step 5 of the instructions). If the control computer is used as a target, all preparation steps must be completed.

To prepare target computers for deployment:

1. Make sure that the following conditions are met:

   - Target computers meet the hardware and software requirements, as well as the requirements for devices with Oracle Linux, Astra Linux, Ubuntu, RED OS, and MosOS operating systems. When deploying KUMA in Kubernetes, the device requirements are satisfied.

     When installing on Astra Linux, you must provide the user with a high level of integrity. To do it, run the command:

     ```
     sudo pdpl-user -i 63 <user that will be installing the solution>
     ```

   - The network ports required by KUMA during installation are available.

2. Disable the SELinux module:

   a. Open the configuration file:

   ```
   sudo vi /etc/selinux/config
   ```

b. Find the following string:

```
SELINUX=enforcing
```

c. Change the parameter value to `disabled`:

```
SELINUX=disabled
```

d. Save changes and exit the editor.

e. Restart the server:

```
sudo reboot
```

3. Specify the host name. We recommend specifying the fully qualified domain name (FQDN), for example `kuma1.example.com`:

```
sudo hostnamectl set-hostname kuma1.example.com
```

The hostname is used when generating the inventory file. The host name can begin with a numeral if this is consistent with the naming scheme adopted at the organization. However, for KUMA services to work with Raft, a host name may not start with a numeral.

If your host name starts with a numeral, you do not need to rename the server. Configure an additional name that starts with a letter by following these steps:

a. In the `/etc/hosts` file, add a line:

```
<IP> <new_fqdn> <fqdn> <hostname>
```

where:

`<IP>` is the IP address of the server.

`<new_fqdn>` is the additional host name.

`<fqdn>` is the source FQDN.

`<hostname>` is a short host name.

b. On your DNS server, create a CNAME record in which `<new_fqdn>` points to `<fqdn>`.

If necessary, for single server deployments, distributed deployments, and deployments in a Raft cluster, the hostname can be changed after installing KUMA. The host name will also be used when services issue certificates.

To check and obtain the current host name, run the following command:

```
hostname -f
```

The control computer must be able to access the target computer by this name.

4. Register the hostname on the network. To allow the control computer to connect to the target computers using FQDN, configure host name resolution to IP addresses using one of the following methods:

   - If you are using a DNS server, add records for each target computer to the DNS zone. The configuration of DNS zone settings depends on the implementation of the DNS server used in the infrastructure. To register host names in DNS zones, you need to contact DNS server administrators in your organization.

   - If there is no DNS server, you can use the `/etc/hosts` file to resolve host names. The `/etc/hosts` file must contain entries for all KUMA hosts and be identical or consistent across all target computers.

     When deploying KUMA in a Kubernetes cluster, you cannot use the `/etc/hosts` file.

     Example of /etc/hosts file

     ```
     127.0.0.1       localhost

     # KUMA nodes
     192.168.1.10    kuma-core1.example.com            kuma1
     192.168.1.11    kuma-collector-1.example.com      kuma2
     192.168.1.12    kuma-correlator-1.example.com     kuma3
     ```

     The first column contains the host IP address, the second *contains* the fully qualified domain name (FQDN), and the third *contains* the short host name.

5. Configure time synchronization with the NTP server on all target computers. The following is an example of time synchronization configuration. The implementation of the configuration may vary depending on the operating system used and the selected NTP client (for example, chrony, ntpd, systemd-timesyncd, and others). Select and configure the appropriate option according to your infrastructure.

   a. Install chrony:

   ```
   sudo apt install chrony
   ```

   This example uses the apt package manager found on Debian-based systems (such as Ubuntu). Installation commands may differ for other Linux distributions. Use the appropriate package manager for your system.

   b. Make sure the virtual machine has internet access. If you have access, go to the next step.

   If internet is not accessible, in the `/etc/chrony.conf` file replace the `2.pool.ntp.org` value with the name or IP address of your organization's internal NTP server.

   c. Start the system time synchronization service:

   ```
   sudo systemctl enable --now chrony
   ```

   Execute the following command:

   ```
   sudo timedatectl | grep 'System clock synchronized'
   ```

   If the system time is synchronized correctly, the output will contain `System clock synchronized: yes`.

   Setting up time synchronization with the NTP server is now complete. If your chosen KUMA deployment configuration does not use a Kubernetes cluster, skip the next step.

6. If you plan to deploy in a Kubernetes cluster, make sure the following additional conditions are met on the target computers:

   a. IP addresses from the following Kubernetes blocks are not used, as IP addresses from these blocks are excluded from traffic to proxy servers:

      - serviceCIDR: 10.96.0.0/12
      - podCIDR: 10.244.0.0/16

   b. Each host must have a unique ID stored in the `/etc/machine-id` file.

   c. The hosts support cgroup v2.

      You can check if cgroup v2 is supported on target hosts by running the following command:

      ```
      sudo stat -fc %T /sys/fs/cgroup/
      ```

      Expected response: `cgroup2`.

      If the command returns any other value, the host does not meet the requirements for installing k0s. You need to enable or configure cgroup v2 support in the operating system.

   d. A firewalld or uwf firewall management tool must be installed and enabled on the hosts for adding network filtration rules to iptables.

   e. The NGINX load balancer is installed and configured.

      You can install the load balancer using one of the following commands:

      ```
      For Oracle Linux operating system
      sudo yum install nginx
      ```

      ```
      For Astra Linux operating system
      sudo apt install nginx-full
      ```

      ```
      For Ubuntu operating system
      sudo apt install nginx libnginx-mod-stream
      ```

      ```
      For RED operating system
      sudo yum install nginx nginx-all-modules
      ```

      If you want the NGINX load balancer to be configured automatically during the KUMA installation, install the NGINX load balancer and allow SSH access to it in the same way as for the Kubernetes cluster hosts (see below). For more information, please refer to NGINX documentation.

      Example of an automatically created NGINX configuration

      The installer creates the `/etc/nginx/kuma_nginx_lb.conf` configuration file. An example of the file contents is shown below. The `upstream` sections are generated dynamically and contain the IP addresses of the Kubernetes cluster controllers (in the example 10.0.0.2-4, in the `upstream kubeAPI_backend`, `upstream konnectivity_backend`, `controllerJoinAPI_backend` sections) and the IP addresses of the worker nodes (in the example 10.0.1.2-3), for which the inventory file contains the `"kaspersky.com/kuma-ingress=true"` value for the `extra_args` variable.

The "`include /etc/nginx/kuma_nginx_lb.conf;`" line is added to the end of the `/etc/nginx/nginx.conf` file to apply the generated configuration file. With a large number of active services and users, you may need to increase the limit of open files in the `nginx.conf` settings.

Configuration file example:

```
# Ansible managed
#
# LB KUMA cluster
#

stream {
    server {
        listen          6443;
        proxy_pass      kubeAPI_backend;
    }
    server {
        listen          8132;
        proxy_pass      konnectivity_backend;
    }
    server {
        listen          9443;
        proxy_pass      controllerJoinAPI_backend;
    }
    server {
        listen          7209;
        proxy_pass      kuma-core-hierarchy_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7210;
        proxy_pass      kuma-core-services_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7220;
        proxy_pass      kuma-core-ui_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7222;
        proxy_pass      kuma-core-cybertrace_backend;
        proxy_timeout   86400s;
    }
    server {
        listen          7223;
        proxy_pass      kuma-core-rest_backend;
        proxy_timeout   86400s;
    }
    upstream kubeAPI_backend {
        server 10.0.0.2:6443;
        server 10.0.0.3:6443;
        server 10.0.0.4:6443;
    }
    upstream konnectivity_backend {
        server 10.0.0.2:8132;
        server 10.0.0.3:8132;
        server 10.0.0.4:8132;
    }
    upstream controllerJoinAPI_backend {
        server 10.0.0.2:9443;
        server 10.0.0.3:9443;
        server 10.0.0.4:9443;
    }
    upstream kuma-core-hierarchy_backend {
        server 10.0.1.2:7209;
        server 10.0.1.3:7209;
    }
    upstream kuma-core-services_backend {
        server 10.0.1.2:7210;
        server 10.0.1.3:7210;
    }
    upstream kuma-core-ui_backend {
        server 10.0.1.2:7220;
        server 10.0.1.3:7220;
    }
    upstream kuma-core-cybertrace_backend {
        server 10.0.1.2:7222;
```

```
        server 10.0.1.3:7222;
    }
    upstream kuma-core-rest_backend {
        server 10.0.1.2:7223;
        server 10.0.1.3:7223;
    }
 worker_rlimit_nofile 1000000;
 events {
worker_connections 20000;
}
# worker_rlimit_nofile is the limit on the number of open files (RLIMIT_NOFILE) for workers.This is used to
raise the limit without restarting the main process.
# worker_connections is the maximum number of connections that a worker can open simultaneously.
```

Target computers are ready to deploy KUMA.

Generating keys and configuring access

For the Ansible installer to work correctly when started from the control computer, you need to provide SSH access to the target computers. This is required so that the Ansible installer can connect to servers, copy files, deploy KUMA components, and apply the configuration.

SSH access is configured using authentication keys. Keys allow establishing a connection without entering a password and ensure an encrypted connection between the control and target computers.

Perform the following steps on the control computer:

1. Generate an SSH key pair for authentication on the SSH servers of the target computers:

   ```
   sudo ssh-keygen -f /root/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   As a result, the following keys are created on the control machine:

   - Private key: `/root/.ssh/id_rsa`
   - Public key: `/root/.ssh/id_rsa.pub`

   If SSH root access is blocked on the control computer, generate an SSH key pair for authentication on the SSH servers of the target computers using a user from the sudo group:

   ```
   ssh-keygen -f /home/<name of the user from the sudo group>/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```

   This saves the keys in the .ssh directory in the home directory of the specified user.

   If the SSH key is stored at a path other than that specified in the generation command, specify the full path to the private key on the control machine in the `ansible_ssh_private_key_file` setting in the `kuma: vars:` section of the inventory file. Ansible will use this key to connect to target machines.

2. Make sure that the control machine has network access to all target machines by hostname.

3. Configure authentication with an SSH key on each target machine:

   - If the root user is used for the connection, copy the `/root/.ssh/id_rsa.pub` public SSH key from the control machine and add it to the `/root/.ssh/authorized_keys` file on each target machine (including the control machine if the control machine plays the role of a target machine).

     ```
     sudo ssh-copy-id -i /root/.ssh/id_rsa.pub root@<target machine host name>
     ```

   - If the root user is used for the connection, copy the `/home/<user name>/.ssh/id_rsa.pub` public SSH key from the control machine and add it to the `/home/<user name>/.ssh/authorized_keys` file on each target machine (including the control machine if the control machine plays the role of a target machine).

     ```
     ssh-copy-id -i /home/<user name>/.ssh/id_rsa.pub <user name>@<target machine host name>
     ```

   The private key (`/root/.ssh/id_rsa` or `/home/<user name>/.ssh/id_rsa`) must remain on the control machine.

   Private SSH keys are stored on the control machine, and a corresponding public key is added to `authorized_keys` on each target machine. The private key is not copied to target machines.

4. Test the connection to each target machine:

   - If connecting as root:

     ```
     ssh root@<target machine host name>
     ```

   - If connecting as a user from the sudo group:

     ```
     ssh <user name>@<target machine host name>
     ```

   After successful authentication, an SSH session is opened on the target machine.

The preparation stage is completed. You can proceed with installing KUMA depending on the selected configuration type:

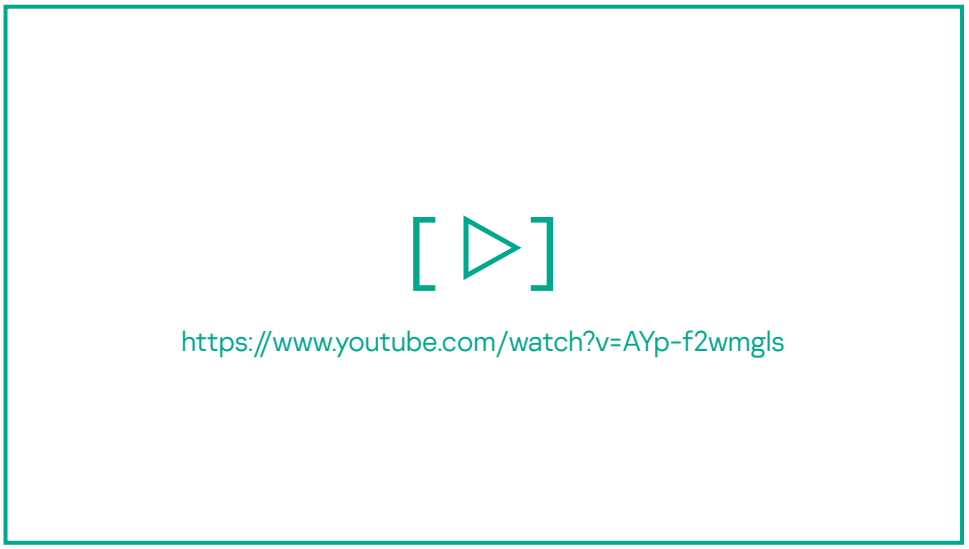
- Installing KUMA on a single server;
- Installing KUMA in a distributed configuration;
- Installation in high availability configuration with KUMA Core in a Kubernetes cluster;
- Installation in high availability configuration with KUMA Core in a Raft cluster.

Installation on a single server

These instructions are part of the deployment and initial configuration scenario.

The installation is performed from the control computer, and all of the solution's components are installed on target computers.

To learn more about installing Kaspersky SIEM on a single server, watch the video below, and then follow the step-by-step instructions.



Before starting the installation, make sure that you have completed the preparation steps. Also make sure you have a valid license key to activate the solution.

To install Kaspersky SIEM on a single server, go to the control computer and do the following:

1 Place the installer archive on the control machine

In your account on the Kaspersky CompanyAccount portal, download the installer archive. Then copy the `kuma-ansible-installer-<KUMA version number>.tar.gz` archive to the control computer and unpack it by using the following command (about 2 GB of disk space is required):

```
tar -xpf kuma-ansible-installer-<KUMA version number>.tar.gz
```

2 Go to the directory with the installer and grant access to files in the directory to the operating system user that is running the KUMA installer.

To do so, run the following sequence of commands:

```
cd kuma-ansible-installer
chown -R <user_name>:<group> kuma-ansible-installer
```

where:

- <user_name> is the operating system user that is running the KUMA installer and needs permissions for the installer directory. This user also needs write permissions for the directory into which the archive will be extracted.
- <group> is the main group of the user.

3 Activate the solution

Depending on the activation method, follow these steps:

- Key file

  Place the `license.key` file in the `<installer directory>/roles/kuma/files/` directory:

  ```
  cp <key file>.key <installer directory>/roles/kuma/files/license.key
  ```

- Activation code

  No action required, proceed to the next step of the instructions.

  > The application can be activated using an activation code only in KUMA 3.4 and later versions. For earlier versions of the solution, activate the application using a key file.

4 Prepare an inventory file

1. Copy the `single.inventory.yml.template` template and create an inventory file named `single.inventory.yml`:

   ```
   cp single.inventory.yml.template single.inventory.yml
   ```

   The template contains a basic set of parameters, but you must not use it for installation without making changes first.

2. Specify the settings in the `single.inventory.yml` file in accordance with your scenario. The possible settings are listed in the table of settings in the inventory file.

   a. Replace `kuma.example.com` with an FQDN in the format `<hostname>.<domain>`. If necessary, specify an IPv4 or IPv6 address.

   b. If you use a non-standard directory for storing SSH keys, specify the full path to the SSH key in the inventory file as the value of the `ansible_ssh_private_key_file` parameter in the `kuma: vars:` section to provide access for the installer to a target computer.

   c. If you want to use a non-standard port for SSH connection during installation, specify the port in the `ansible_port` parameter in the inventory file in the `vars` section.

   d. If you want predefined services (collector, correlator, and storage) to be created during installation, set `deploy_example_services` to `true`.

   Predefined services will be created and automatically started on the hosts specified in the inventory file. The created services will become available in the Kaspersky SIEM web interface. You do not need to install or start these separately. You can remove the predefined services if necessary.

Below is an example of the `single.inventory.yml` inventory file for installing KUMA from the control machine to the target machine, with the full path to the SSH key specified, with the deployment of the predefined collector, correlator, and storage services, and a non-standard port for SSH connections.

Example single.inventory.yml inventory file

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: true
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <full path to the file with the SSH key>
    ansible_user: <user from the sudo group>
    ansible_become: true
    ansible_port: 2222
  children:
    kuma_core:
      hosts:
        kuma1.example.com:
    kuma_collector:
      hosts:
        kuma1.example.com
    kuma_correlator:
      hosts:
        kuma1.example.com
    kuma_storage:
      hosts:
        kuma1.example.com:
          shard: 1
          replica: 1
          keeper: 1
    kuma_metrics:
      hosts:
        kuma1.example.com
```

We recommend saving a backup copy of the inventory file that you used to install the application. You can use it to add components to the system or remove Kaspersky SIEM.

5 Run the installer

Run the `install.sh` installer with the prepared `single.inventory.yml` inventory file:

```
For a user with root rights
```

```
./install.sh single.inventory.yml
```

```
To elevate privileges for a user without root rights, enter a password
```

```
./install.sh single.inventory.yml --ask-become-pass
```

6 Read the terms of the License Agreement

If you do not accept the terms of the End User License Agreement, the solution will not be installed.

If you want to accept the terms of the License Agreement, when the command prompt is displayed, enter:

```
yes
```

7 Complete the installation

To complete the installation, do the following depending on the activation method of the solution:

Key file

If you are activating the solution using a key file and have placed the key file to the `<installer directory>/roles/kuma/files/` directory, running the installer with the `single.inventory.yml` inventory file installs the KUMA Core and Metrics services. On the specified hosts listed in the inventory file, the files required for further installation and start of KUMA services are deployed, and pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix are available.

Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

After the installer finishes, log in to the web interface.

Activation code

If you activate the solution using an activation code, only the KUMA Core and the Metrics service will be installed.

To complete the installation:

1. Log in to the web interface and enter an activation code.
2. Then run the `postinstall.sh` installer with the `single.inventory.yml` inventory file:

   ```
   ./postinstall.sh single.inventory.yml
   ```

   The hosts specified in the inventory file contain the files required for further installation and start of KUMA services. Pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix will be available for import in the repository.

   Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

The installation is complete. You can return to the deployment script and continue from the Post-installation steps. If necessary, the configuration can be scaled to a distributed one.

Installation in a distributed configuration

These instructions are part of the deployment and initial configuration scenario.

The installation is performed from the control computer, and all of the solution's components are installed on target computers.

To learn more about installing Kaspersky SIEM in a distributed configuration, watch the video below, and then follow the step-by-step instructions.

Before starting the installation, make sure that you have completed the preparation steps. Also make sure you have a valid license key to activate the solution.

To install Kaspersky SIEM in a distributed configuration, go to the control computer and do the following:

1. Place the installer archive on the control computer

In your account on the Kaspersky CompanyAccount portal, download the installer archive. Then copy the `kuma-ansible-installer-<KUMA version number>.tar.gz` archive to the control computer and unpack it by using the command (about 2 GB of disk space is required):

```
tar -xpf kuma-ansible-installer-<KUMA version number>.tar.gz
```

2. Go to the directory with the installer and grant access to files in the directory to the operating system user that is running the KUMA installer.

To do so, run the following sequence of commands:

```
cd kuma-ansible-installer
chown -R <user_name>:<group> kuma-ansible-installer
```

where:

- <user_name> is the operating system user that is running the KUMA installer and needs permissions for the installer directory. This user also needs write permissions for the directory into which the archive will be extracted.
- <group> is the main group of the user.

3 Activate the solution

Depending on the activation method, follow these steps:

- Key file

  Place the `license.key` file in the `<installer directory>/roles/kuma/files/` directory:

  ```
  cp <key file>.key <installer directory>/roles/kuma/files/license.key
  ```

- Activation code

  No action required, proceed to the next step of the instructions.

  > The application can be activated using an activation code only in KUMA 3.4 and later versions. For earlier versions of KUMA, you must activate the application with a key file.

4 Prepare an inventory file

1. Create an inventory file named `distributed.inventory.yml` by copying the `distributed.inventory.yml.template` template:

   ```
   cp distributed.inventory.yml.template distributed.inventory.yml
   ```

   The template contains a basic set of parameters, but you must not use it for installation without making changes first.

2. Specify the settings in the `distributed.inventory.yml` file in accordance with your scenario. The possible settings are listed in the table of settings in the inventory file.

   a. The `distributed.inventory.yml` inventory template provides examples of host names for different KUMA service groups. Before installation, replace these examples with valid FQDNs in the <host name>.<domain> format and, if necessary, specify the IPv4 or IPv6 addresses of the infrastructure servers where the corresponding services will be installed.

   b. If you use a non-standard directory for storing SSH keys, specify the full path to the SSH key in the `ansible_ssh_private_key_file` setting in the `kuma:vars` section of the the inventory file to make sure the installer can gain access to target machines.

c. If you want to use a non-standard port for the SSH connection during installation, select one of the following options:

- If the port is the same for a group of hosts, specify the port in the `ansible_port` parameter of the inventory file's `vars` section.
- If a different non-standard port is used to connect to each host, specify the port in the `ansible_port` parameter for each host in the inventory file.

d. If you want predefined services (collector, correlator, and storage) to be created during installation, set `deploy_example_services` to `true`.

   Predefined services will be created and automatically started on the hosts specified in the inventory file. The created services will become available in the Kaspersky SIEM web interface. You do not need to install or start these separately. You can remove the predefined services if necessary.

Below is an example of how to fill in the `distributed.inventory.yml` inventory file. The example shows the full path to the SSH key, without deploying predefined services, and with a separate non-standard SSH port for the collector and correlator, and common non-standard port for the storage host group.

Example of the distributed.inventory.yml inventory file

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <full path to the file with the SSH key>
    ansible_user: <user from the sudo group>
    ansible_become: true
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          raft_node_addr: ""
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ansible_port: 2223
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2224
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
```

```
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

We recommend saving a backup copy of the inventory file that you used to install the application. You can use it to add components to the system or remove KUMA.

5 Run the installer

Run the `install.sh` installer with the prepared `distributed.inventory.yml` inventory file:

```
For a user with root rights
./install.sh distributed.inventory.yml
```

```
To elevate privileges for a user without root rights, a password is required
./install.sh distributed.inventory.yml --ask-become-pass
```

6 Read the terms of the License Agreement

If you do not accept the terms of the End User License Agreement, the solution will not be installed.

If you want to accept the terms of the License Agreement, when the command prompt is displayed, enter:

```
yes
```

7 Complete the installation

To complete the installation, do the following depending on the activation method of the solution:

Key file

If you are activating the solution using a key file and have placed the key file to the directory `<installer directory>/roles/kuma/files/`, running the installer with the `distributed.inventory.yml` inventory file installs KUMA Core and the Metrics services. On the specified hosts listed in the inventory file, the files required for further installation and start of KUMA services are deployed, and pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix are available.

Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

After the installer finishes, log in to the web interface.

Activation code

If you activate the solution using an activation code, only the KUMA Core and the Metrics service will be installed.

To complete the installation:

1. Log in to the web interface and enter an activation code.
2. Run the `postinstall.sh` installer with the `distributed.inventory.yml` inventory file:

   ```
   ./postinstall.sh distributed.inventory.yml
   ```

   The hosts specified in the inventory file contain the files required for further installation and start of KUMA services. Pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix will be available for import in the repository.

   Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

The installation is complete. You can return to the deployment script and continue from the Post-installation steps.

Installing in a high availability configuration in a Kubernetes cluster

These instructions are part of the deployment and initial configuration scenario.

The installation is performed from the control computer, and all of the solution's components are installed on target computers.

> Before starting the installation, make sure that you have completed the preparation steps. Also make sure you have a valid license key to activate the solution.

To install Kaspersky SIEM in a Kubernetes cluster, go to the control computer and do the following:

1 Place the installer archive on the control computer

In your account on the Kaspersky CompanyAccount portal, download the installer archive. Then copy the `kuma-ansible-installer-ha-<KUMA version number>.tar.gz` archive to the control computer and unpack it by using the following command (about 2 GB of disk space is required):

```
tar -xpf kuma-ansible-installer-ha-<KUMA version number>.tar.gz
```

2 Go to the directory with the installer and grant access to files in the directory to the operating system user that is running the KUMA installer.

To do so, run the following sequence of commands:

```
cd kuma-ansible-installer
chown -R <user_name>:<group> kuma-ansible-installer
```

where:

- <user_name> is the operating system user that is running the KUMA installer and needs permissions for the installer directory. This user also needs write permissions for the directory into which the archive will be extracted.
- <group> is the main group of the user.

3 Activate the solution

Depending on the activation method, follow these steps:

- Key file

  Place the `license.key` file in the `<installer directory>/roles/kuma/files/` directory:

  ```
  cp <key file>.key <installer directory>/roles/kuma/files/license.key
  ```

- Activation code

  No action required, proceed to the next step of the instructions.

4 Prepare an inventory file

1. Copy the `k0s.inventory.yml.template` template, and create an inventory file named `k0s.inventory.yml`:

   ```
   cp k0s.inventory.yml.template k0s.inventory.yml
   ```

   The template contains a basic set of parameters, but you must not use it for installation without making changes first.

2. Specify the settings in the `k0s.inventory.yml` file in accordance with your scenario. The possible settings are listed in the table of settings in the inventory file.

   a. The `k0s.inventory.yml` inventory file template provides examples of host names for different KUMA service groups. Before installation, replace these examples with valid FQDNs in the <host name>.<domain> format and, if necessary, specify the IPv4 or IPv6 addresses of the infrastructure servers where the corresponding services will be installed.

   b. If you use a non-standard directory for storing SSH keys, specify the full path to the SSH key in the `ansible_ssh_private_key_file` parameter in the inventory file in the `kuma: vars:` section to provide access for the installer to target computers.

   c. If you want to use a non-standard port for the SSH connection during installation, select one of the following options:

      - If the port is the same for a group of hosts, specify the port in the `ansible_port` parameter of the inventory file's `vars` section.

      - If a different non-standard port is used to connect to each host, specify the port in the `ansible_port` parameter for each host in the inventory file.

   d. If you want predefined services (collector, correlator, storage) to be created during installation, set `deploy_example_services` to `true`.

      Predefined services will be created and automatically started on the hosts specified in the inventory file. The created services will become available in the Kaspersky SIEM web interface. You do not need to install or start these separately. You can remove the predefined services if necessary.

   e. In the inventory file for the worker node that will be used for access to KUMA Core, specify `kaspersky.com/kuma-ingress=true` in the `extra_args` setting. Use an URL in the following format ofr access to the KUMA Core: `https: // <FQDN of the worker node>:<port of the worker node>`. Port 7220 is the default port for connecting to the web interface. Available ports: 7209, 7210, 7220, 7222, 7223.

      The `extra_args` setting can be specified for multiple nodes. You cannot connect to the Kaspersky SIEM web interface on multiple worker nodes at the same time using the same credentials. Only the last established connection remains active.

      If you are using an external load balancer in a high availability Kubernetes cluster configuration, the ports of the KUMA Core are accessed via the FQDN of the load balancer.

Below is an example of how to fill in the `k0s.inventory.yml` inventory file with three controllers, two worker nodes, and one balancer. The example also shows the full path to the SSH key, without deploying pre-installed services, and with a separate non-standard SSH port for the collector and correlator, and common non-standard port for the storage host group.

An example of an inventory file for installation in a highly available configuration in a Kubernetes cluster

```
all:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <full path to the SSH key file>
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
          ansible_port: 2221
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2223
      hosts:
        kuma-storage-cluster1.server1.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server2.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server3.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server4.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server5.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server6.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1.server7.example.com:
          ip: 0.0.0.0
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          ip: 0.0.0.0
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp2.example.com:
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
        kuma-w1.example.com:
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-
ingress=true,node.longhorn.io/create-default-disk=true"
```

We recommend saving a backup copy of the inventory file that you used to install the application. You can use it to add components to the system or remove KUMA.

5 Run the installer

Run the `install.sh` installer with the prepared `k0s.inventory.yml` inventory file:

```
For a user with root rights

./install.sh k0s.inventory.yml
```

```
To elevate privileges for a user without root rights, a password is required

./install.sh k0s.inventory.yml --ask-become-pass
```

During Kaspersky SIEM installation, the hosts are automatically checked to see if they meet hardware requirements.

If these conditions are not satisfied, the installation is stopped. For a demo installation, you can disable checking the hardware requirements by setting a variable in the inventory file:

```
low_resources: true
```

6 Read the terms of the License Agreement

If you do not accept the terms of the End User License Agreement, the solution will not be installed.

If you want to accept the terms of the License Agreement, when the command prompt is displayed, enter:

```
yes
```

7 Complete the installation

To complete the installation, do the following depending on the activation method of the solution:

Key file

If you are activating the solution using a key file and have placed the key file to the directory `<installer directory>/roles/kuma/files/`, running the installer with the `k0s.inventory.yml` inventory file installs KUMA Core and the Metrics service. On the specified hosts listed in the inventory file, the files required for further installation and start of KUMA services are deployed, and pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix are available.

Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

When installing Kaspersky SIEM on cluster nodes, the k0s utility is automatically installed. The utility allows you to deploy a Kubernetes cluster. The administrator can use the k0s utility to monitor and manage the cluster. After installation, the `artifacts/k0s-kubeconfig.yml` file is created in the installer directory. This file contains the details required for connecting to the Kubernetes cluster. The same file is created on the main controller in the home directory of a user, specified as `ansible_user` in the inventory file.

> To monitor and manage the Kubernetes cluster, the `k0s-kubeconfig.yml` file should be saved in a location available for the cluster administrators. Access to the file must be restricted.

After the installer finishes, log in to the web interface.

Activation code

If you activate the solution using an activation code, only the KUMA Core and the Metrics service are installed.

When installing Kaspersky SIEM on cluster nodes, the k0s utility is automatically installed. The utility allows you to deploy a Kubernetes cluster. The administrator can use the k0s utility to monitor and manage the cluster. A file named `artifacts/k0s-kubeconfig.yml` is created in the installer directory. This file contains the details required for connecting to the created Kubernetes cluster. The same file is created on the main controller in the home directory of a user, specified as `ansible_user` in the inventory file.

> To monitor and manage the Kubernetes cluster, the `k0s-kubeconfig.yml` file should be saved in a location available for the cluster administrators. Access to the file must be restricted.

To complete the installation:

1. Log in to the web interface and enter an activation code.
2. Run the `postinstall.sh` installer with the `k0s.inventory.yml` inventory file:

   ```
   ./postinstall.sh k0s.inventory.yml
   ```

   The hosts specified in the inventory file contain the files required for further installation and start of KUMA services. Pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix will be available for import in the repository.

   Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

The installation is complete. You can return to the deployment script and continue from the Post-installation steps.

Installing in a high availability configuration in a Raft cluster

These instructions are part of the deployment and initial configuration scenario.

The installation is performed from the control computer, and all of the solution's components are installed on target computers.

Before starting the installation, make sure that you have completed the preparation steps. Also make sure you have a valid license key to activate the solution.

To install Kaspersky SIEM in a distributed configuration with the KUMA Core in the Raft cluster, go to the control computer and do the following:

1 Place the installer archive on the control machine

In your account on the Kaspersky CompanyAccount portal, download the installer archive. Then copy the `kuma-ansible-installer-<KUMA version number>.tar.gz` archive to the control computer and unpack it by using the following command (about 2 GB of disk space is required):

```
tar -xpf kuma-ansible-installer-<KUMA version number>.tar.gz
```

2 Go to the directory with the installer and grant access to files in the directory to the operating system user that is running the KUMA installer.

To do so, run the following sequence of commands:

```
cd kuma-ansible-installer
chown -R <user_name>:<group> kuma-ansible-installer
```

where:

- <user_name> is the operating system user that is running the KUMA installer and needs permissions for the installer directory. This user also needs write permissions for the directory into which the archive will be extracted.
- <group> is the main group of the user.

3 Activate the solution

Depending on the activation method, follow these steps:

- Key file

  Place the `license.key` file in the `<installer directory>/roles/kuma/files/` directory:

  ```
  cp <key file>.key <installer directory>/roles/kuma/files/license.key
  ```

- Activation code

  No action required, proceed to the next step of the instructions.

> The application can be activated using an activation code only in KUMA 3.4 and later versions. For earlier versions of KUMA, you must activate the application with a key file.

4 Prepare an inventory file

1. Create an inventory file named `distributed.inventory.yml` by copying the `distributed.inventory.yml.template` template:

   ```
   cp distributed.inventory.yml.template distributed.inventory.yml
   ```

   The template contains a basic set of parameters, but you must not use it for installation without making changes first.

2. Edit the `distributed.inventory.yml` inventory file settings:

   a. The `distributed.inventory.yml` inventory template provides examples of host names for different KUMA service groups. Before installation, replace these examples with valid FQDNs in the `<host name>.<domain>` format and, if necessary, specify the IPv4 or IPv6 addresses of the infrastructure servers where the corresponding services will be installed.

   b. If you use a non-standard directory for storing SSH keys, specify the full path to the SSH key in the `ansible_ssh_private_key_file` parameter in the inventory file in the `kuma:vars` section to provide access for the installer to target computers.

   c. If you want to use a non-standard port for the SSH connection during installation, select one of the following options:

      - If the port is the same for a group of hosts, specify the port in the `ansible_port` parameter of the inventory file's `vars` section.

      - If a different non-standard port is used to connect to each host, specify the port in the `ansible_port` parameter for each host in the inventory file.

   d. If you want predefined services (collector, correlator, storage) to be created during installation, set `deploy_example_services` to `true`.

      Predefined services will be created and automatically started on the hosts specified in the inventory file. The created services will become available in the Kaspersky SIEM web interface. You do not need to install or start these separately. You can remove the predefined services if necessary.

Below is an example of filling out the `distributed.inventory.yml` inventory file. It includes the full path to the SSH key, without deploying of the predefined services. It specifies a common non-standard SSH port for additional KUMA Core hosts, a separate non-standard SSH port for the collector and correlator, and a common non-standard SSH port for the storage host group.

An example of the distributed.inventory.yml inventory file for installation in a highly available configuration in a Kubernetes cluster

```yaml
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
          raft_node_addr: ""
          ansible_port: 2222
    kuma_core_peers:
      vars:
        ansible_port: 2222
      hosts:
        kuma-core-2.example.com:
          ip: 0.0.0.0
        kuma-core-3.example.com:
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
          ansible_port: 2223
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ansible_port: 2224
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ansible_port: 2225
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2226
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
```

```
            shard: 0
            replica: 0
            keeper: 3
```

We recommend backing up the inventory file that you used to install the solution. With its help, you can add components to the solution, update, or remove Kaspersky SIEM.

5 Run the installer

Run the `install.sh` installer with the prepared `distributed.inventory.yml` inventory file:

```
For a user with root rights
./install.sh distributed.inventory.yml
```

```
To elevate privileges for a user without root rights, a password is required
./install.sh distributed.inventory.yml --ask-become-pass
```

6 Read the terms of the License Agreement

If you do not accept the terms of the End User License Agreement, the solution will not be installed.

If you want to accept the terms of the License Agreement, when the command prompt is displayed, enter:

```
yes
```

7 Complete the installation

To do this, complete the following steps:

1. To complete the installation, do the following depending on the activation method of the solution:

   Key file

   If you activate the solution using a key file and place the key file in the `<installer directory>/roles/kuma/files/` directory, running the installer with the `distributed.inventory.yml` inventory file, installs the KUMA Core on the server specified in the `kuma_core` section, additional KUMA Cores on the servers specified in the `kuma_core_peers` section, and the Metrics service on the server specified in the `kuma_metrics` section. On the specified hosts listed in the inventory file, the files required for further installation and start of KUMA services are deployed, and pre-configured resources (normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix are available.

   Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

After the installer finishes, log in to the web interface.

Activation code

If you activate the solution using an activation code, only KUMA Core on the server from the `kuma_core` section, additional KUMA Cores on the servers from the `kuma_core_peers` section, and Metrics service are installed.

To complete the installation:

1. Log in to the web interface and enter an activation code.

2. Run the `postinstall.sh` installer with the `distributed.inventory.yml` inventory file:

   ```
   ./postinstall.sh distributed.inventory.yml
   ```

   The hosts specified in the inventory file contain the files required for further installation and start of KUMA services. Pre-configured resources (such as normalizers, correlation rules, active lists, and others) marked with the **[OOTB]** prefix are available for import into the repository.

   Information about the installation progress, successfully completed operations, and encountered errors is logged only in the KUMA Core logs, which are stored in the `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` directory.

2. Determine whether you will use the balancer for the Raft cluster and, if necessary, configure the balancer:

   - If the balancer is not used, you have to specify the URLs of the KUMA Core nodes separated by commas during the installation of each service. You can to connect to the KUMA Core servers directly. When switching between nodes, re-authentication is required. After successful login on a new node, the session on the previous node will be terminated.

   - The balancer distributes the load among the cluster nodes and provides a single entry point to the web interface (Single Sign-On, SSO) via AD FS, eliminating the need for repeated authentication when switching between cluster nodes. It also ensures continued access to Kaspersky SIEM if one or more hosts running the KUMA Core service are unavailable or down.

     We recommend using one of the following balancers:

     HAProxy Community Edition

     This article provides an example for configuration of the HAProxy Community Edition. If necessary, you can change the settings to suit your needs. This configuration was tested with package version 2.4.24-0ubuntu0.22.04.2.

     To configure HAProxy Community Edition:

     1. On the host where you are installing the balancer, start the command line console and install the `haproxy` package:

        ```
        sudo apt update && sudo apt install haproxy -y
        ```

     2. Go to the `/etc/haproxy` directory, and edit the `haproxy.conf` configuration file as shown in the example. The order of sections and parameters in the configuration file is significant and must be the same as in the example.

Example of settings in the haproxy.cfg file if a TLS certificate is not used

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy

defaults
        log     global
        mode    tcp
        option  tcplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http

frontend deploy-raft
    mode tcp
    bind *:7220
    default_backend be_d1

backend be_d1
    mode tcp
    balance roundrobin
    server machine2 kuma-inst-02.avp.ru:7220 check
    server machine3 kuma-inst-03.avp.ru:7220 check
    server machine4 kuma-inst-04.avp.ru:7220 check
```

Example of settings in the haproxy.cfg file when using a TLS certificate

```
global #
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
# Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private

        ssl-default-bind-ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
        ssl-default-bind-ciphersuites TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
        ssl-default-bind-options ssl-min-ver TLSv1.3 no-tls-tickets

defaults #
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http

frontend http_front
   bind 0.0.0.0:443 ssl crt kuma-inst-01.avp.ru
   default_backend be_d1 #name of the default application server group
```

```
backend be_d1 #be_d1 is the name of the application server group; used by the frontend section for
addressing purposes
   balance roundrobin #requests are distributed equally among available application servers
   cookie SERVER insert indirect nocache #the insert parameter creates a cookie file upon request;
indirect deletes the cookie file upon every incoming request before forwarding it to the application
server, #nocache ensures that there is no caching between the client and the balancer
   option httpchk #start HTTP check
   http-check connect port 7220 #port 7220 is used for the HTTP check
   http-check send meth GET #HTTP method GET is used for the check
   http-check expect status 200 #a successful HTTP check gets the 200 OK status from the application
server
   server machine2 kuma-inst-02.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none #the inter parameter
sets the http-check interval to four seconds to exclude the machine
   server machine3 kuma-inst-03.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none #from the rotation, 2
consecutive checks must fail - fall 2, to return, 4 must
   server machine4 kuma-inst-04.avp.ru:7220 inter 4s fall 2 rise 4 ssl verify none #complete
successfully - rise 4. The authenticity of the server TLS certificate is not verified - ssl  #verify
none
```

3. Save the `haproxy.cfg` configuration file.

4. Check the correctness of the `haproxy.cfg` configuration file using the following command:

   ```
   haproxy -f /etc/haproxy/haproxy.cfg -c
   ```

   If the check command returns an error, make sure the contents of the `haproxy.cfg` configuration file matches the example and make changes if necessary.

   If the check command does not return any errors, proceed to starting the balancer.

5. Start the balancer:

   ```
   sudo systemctl start haproxy
   ```

   If the `haproxy` service needs to be enabled before starting, run the following sequence of commands:

   ```
   sudo systemctl enable haproxy
   ```

   ```
   sudo systemctl start haproxy
   ```

The HAProxy Community Edition balancer is configured.

NGINX Open Source

This article provides an example configuration for NGINX Open Source. If necessary, you can change the settings to suit your needs. This configuration was tested with package version 1.18.0-6ubuntu14.6.

It is recommended to use a load balancer configuration without TLS termination on the NGINX side. In this mode, NGINX acts as a proxy server at the transport layer (TCP) and redirects encrypted traffic to nodes running the KUMA Core service.

TLS termination occurs on the KUMA Core node, so the web interface certificate is installed in KUMA rather than in NGINX. This mode provides end-to-end encryption of traffic between the client and the KUMA Core service.

You can use a TLS certificate that is automatically generated by KUMA during the first start. To avoid browser warnings, it is recommended to use a certificate issued by a corporate or public certification authority and specify the DNS name of the load balancer, as well as the DNS names of all nodes running the KUMA Core service, in the `Subject Alternative Names` (SAN) field. Instead of listing individual names, you can use a wildcard character, such as `*.example.com`.

To configure NGINX Open Source:

1. On the host where you are installing the balancer, start the command line console and install the `nginx-common` package:

   ```
   sudo apt update && sudo apt install nginx-common -y
   ```

2. Go to the `/etc/nginx` directory, and edit the `nginx.conf` configuration file as shown in the example. The order of sections and parameters in the configuration file is significant and must be the same as in the example.

   Example of settings in the nginx.conf file if a TLS certificate is not used

   ```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;
   error_log /var/log/nginx/error.log;
   include /etc/nginx/modules-enabled/*.conf;

   events {
           worker_connections 768;
   }

   http {
           sendfile on;
           tcp_nopush on;
           types_hash_max_size 2048;
           server_tokens off;
           server_name_in_redirect off;

           include /etc/nginx/mime.types;
           default_type application/octet-stream;

           access_log /var/log/nginx/access.log;

           gzip on;

           include /etc/nginx/conf.d/*.conf;
           include /etc/nginx/sites-enabled/*;
   }

   stream {
       include /etc/nginx/stream-conf.d/*.conf;

           upstream backend {
               server kuma-inst-02.avp.ru:7220;
               server kuma-inst-03.avp.ru:7220;
               server kuma-inst-04.avp.ru:7220;
           }

           server {
               listen 7220;
               proxy_pass backend;
           }
   }
   ```

   Example of settings in the nginx.conf file when using a TLS certificate

   ```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;
   include /etc/nginx/modules-enabled/*.conf;
   ```

```
events {
        worker_connections 768;
}

http {

        ##
        # Basic Settings
        ##

        sendfile on;
        tcp_nopush on;
        types_hash_max_size 2048;
        server_tokens off;

        server_name_in_redirect off;

        include /etc/nginx/mime.types;
        default_type application/octet-stream;

        ##
        # Logging Settings
        ##

        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;

        ##
        # Gzip Settings
        ##

        gzip on; #

        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;


    server {
        listen              443 ssl;
        server_name         kuma-inst-01.avp.ru;
        ssl_certificate     kuma-inst-01.avp.ru;
        ssl_certificate_key kuma-inst-01.avp.ru.key;
        ssl_protocols       TLSv1.3;
        ssl_ciphers         HIGH:!aNULL:!MD5;

        location / { #path that is accessed to pass requests to the group of servers from proxy_pass
            proxy_pass https://Kuma-UI; #proxy_pass - the directive for passing requests to the Kuma-UI
server group
        }
    }

    ##
#max_fails—the number of failed solution server availability checks within the interval.
#fail_timeout - the time after which the computer is excluded from balancing.
    ##

    upstream Kuma-UI {
        hash $request_uri consistent;
        server kuma-inst-02.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-03.avp.ru:7220 max_fails=1 fail_timeout=30s;
        server kuma-inst-04.avp.ru:7220 max_fails=1 fail_timeout=30s;
    }
}
```

3. Save the `nginx.conf` configuration file.

4. Check the correctness of the `nginx.cfg` configuration file using the following command:

```
sudo nginx -f /etc/nginx/nginx.conf -t
```

If the check command returns an error, make sure the contents of the `nginx.conf` configuration file matches the example, and make changes if necessary.

If the check command does not return any errors, proceed to starting the balancer.

5. Start the balancer:

```
sudo systemctl start nginx
```

If the `nginx` service needs to be enabled before starting, run the following sequence of commands:

```
sudo systemctl enable nginx
```

```
sudo systemctl start nginx
```

The NGINX Open Source balancer is configured.

3. If you have configured the use of a load balancer, enable domain authentication via AD FS if necessary:

   a. Specify the FQDN of the balancer in the AD FS settings.

   b. In Kaspersky SIEM, configure domain authentication via AD FS by specifying the FQDN of the balancer in the settings.

4. Set the same time zone on all servers on which the KUMA Core services are deployed. After the installation is complete, you can change the time zone, if necessary; the changes must be applied simultaneously to all nodes of the Raft cluster.

The installation is complete. You can return to the deployment script and continue from the Post-installation steps.

Configuring exclusions in Kaspersky Endpoint Security for Linux

When installing KUMA components and Kaspersky Endpoint Security for Linux on the same server, the following issues may occur:

- The report.db directory can become large and take up all disk space.
- Scanning all KUMA files, including service files, with Kaspersky Endpoint Security for Linux may decrease system performance.
- Interception or blocking of network traffic used by KUMA components can disrupt their interaction.

To avoid these problems:

1. Upgrade Kaspersky Endpoint Security for Linux to version 12.0 or later.
2. Configure the components of Kaspersky Endpoint Security for Linux in accordance with the recommendations below.

Recommended settings for Kaspersky Endpoint Security for Linux

Application component	Recommended setting
File Threat Protection	Enabled Add the `/opt/kaspersky/kuma` directory to general exclusions and exclusions for the on-demand scan.
Behavior Detection	Enabled Exclude the `/opt/kaspersky/kuma/kuma` process from scanning.
Container Monitoring	Enabled
Web Threat Protection	Enabled
Network Threat Protection	Enabled Disable blocking of a compromised device `BlockAttackingHosts=No.`
Firewall Management	Enabled
System Integrity Monitoring	Enabled
Application Control	Disabled
Web Control	Disabled
Mail Threat Protection (Mail AV)	Disabled
Bad USB Attack Protection	Disabled

The exclusion for the `/opt/kaspersky/kuma` directory applies to the entire KUMA directory and its contents. Therefore, when adding new KUMA components or service directories, additional exclusions for individual directories are not needed.

For more details on scan exclusions, please refer to the Kaspersky Endpoint Security for Linux Online Help.

Configuring exclusions for a KUMA instance in a high-availability configuration

For a KUMA instance deployed in a high-availability (HA) configuration, configure the following exclusions:

- Add TCP traffic from and to port 443 of the internal Kubernetes API Service to KESL exclusions. By default, a KUMA instance with k0s uses 10.96.0.1:443 as the address and port. KESL intercepting or blocking this HTTPS traffic can disrupt the interaction of cluster components with Kubernetes API and interfere with Calico CNI, which can lead to errors when running pods and disrupt the cluster.

  The 10.96.0.1 IP address is the default value of `ClusterIP` and may differ depending on the specific cluster configuration. To get your current `ClusterIP`, on the node with the controller role, run the following command:

  ```
  k0s kubectl get svc kubernetes -n default -o jsonpath='{.spec.clusterIP}{"\n"}'
  ```

  Use the obtained `ClusterIP` value to configure an exclusion for TCP traffic on port 443.

- Add the Kubernetes mount point to the general exclusions:

  ```
  /var/lib/k0s/kubelet/pods
  ```

Logging in to the web interface

Only users with *Active* user account status can log in to the solution web interface.

KUMA does not allow creating multiple sessions for a user at the same time. If you try to log in to the web interface again, for example, from another browser, the earlier session is automatically terminated.

We recommend using the security policy to configure password requirements and rules for logging in to the solution web interface.

To log in to the solution web interface:

1. Enter the following address in your browser:

   ```
   https://<IP address or FQDN of KUMA Core server>:7220
   ```

   The web interface authorization page will open and prompt you to enter your login and password.

2. Enter the login of your local account in the **Login** field.

   When authenticating with a domain account, you need to specify a `UserPrincipalName` (for example, `user@domain.ru`).

3. Enter the password for the specified account in the **Password** field.

   Default login credentials:

   Login
   ```
   admin
   ```

   Password
   ```
   mustB3Ch@ng3d!
   ```

   After the first login, change the password of the admin account.

4. Click the **Sign in** button.

   If you enter incorrect credentials, you can try to log in again after three seconds. This delay helps prevent an attacker from brute-forcing a password to log in to the web interface. If you enter incorrect credentials several times in a row, your user account becomes blocked. The maximum number of failed login attempts and the account lockout duration are governed by the security policy. The default value is 0, which means that the check for the maximum number of failed attempts is disabled.

The main window of the solution web interface is displayed.

In multi-tenancy mode, a user logging in to the solution web interface for the first time is shown data only for those tenants that were selected for this user when their account was created.

After logging in, you can select a language and an interface theme. Russian and English languages are available, as well as a light and a dark theme. The light theme is selected by default. The selected language and theme are applied to all sections of the web interface of the solution and persist across KUMA sessions until you change them.

The date display format depends on the selected interface language. The following date formats are possible:

- English UI language: YYYY-MM-DD.
- Russian UI language: DD.MM.YYYY.

To change the UI language:

1. In the lower left corner of the web interface, click the account name.
2. In the user account menu that is displayed, click the **English** or **Русский** button.

To change the UI theme:

1. In the lower left corner of the web interface, click the account name.
2. In the user account menu that is displayed, click the **Light** or **Dark** button.

While managing the solution web interface, you can use shortcut keys to perform the following actions:

- In all sections: close the window that opens in the right side pane by pressing **`Esc`**.
- In the **Events** section:
  - Switch between events in the right side pane—↑ and ↓.
  - Start a search (when focused on the query field)—**`Ctrl/Command`**+**`Enter`**.
  - Save a search query—**`Ctrl/Command`**+**`S`**.

To log out from the solution web interface:

1. In the lower left corner of the web interface, click the account name.
2. In the opened account menu, click the **Logout** button.

Administration

This Help section provides instructions for configuring and maintaining a previously deployed KUMA solution.

Updating

This section contains articles that relate to updating KUMA from previous versions.

If your infrastructure has tenants that are managed by different teams, see the How to update Kaspersky Unified Monitoring and Analysis Platform when tenants are managed by different teams article.

Updating previous versions of the solution

The upgrade procedure is the same for all hosts and involves using the installer and inventory file.

Upgrade scheme

Versions must be upgraded in accordance with the following scheme:

3.2.x → 3.4.x → 4.0 → 4.2 → 4.6

For certified versions of KUMA, the update is performed sequentially, just like for the regular versions. When upgrading across versions, at intermediate stages, you can use a distribution kit of an uncertified version. You must follow the exact update sequence without skipping any intermediate versions.

> If you manually edited unit files of KUMA services in the `/usr/lib/systemd/system` directory, these changes are lost when upgrading from a previous version of KUMA. If necessary, make these changes again once the solution is upgraded.

Upgrade instructions

Upgrading from version 3.2.0 or 3.2.1 to 3.4

Limitations:

1. For existing users, after upgrading from 3.2.0 or 3.2.1 to 3.4, the universal dashboard layout is not refreshed.

   Possible solution: restart the Core service, `kuma-core.service`. After that, the data will be updated at the interval specified for the layout.

2. If the old Core service, `kuma-core.service` is still displayed after the upgrade, run the following command after installation is complete:

   ```
   sudo systemctl reset-failed
   ```

   After running the command, the old service is no longer displayed, and the new service starts successfully.

Upgrading KUMA from version 3.2.0 or 3.2.1 to version 3.4 involves the following steps:

1 Preliminary steps

1. Make sure that all hardware and software requirements for solution installation are met.

2. Creating a backup copy of the KUMA Core. If necessary, you will be able to restore data from backup for version 3.2.

   KUMA backups created in versions 3.2 and earlier cannot be restored in version 3.4. This means that you cannot install KUMA 3.4 and restore a KUMA 3.2.x backup in it.

   Create a backup copy immediately after upgrading KUMA to version 3.4.

3. Make sure that the host name of the KUMA Core does not start with a numeral. The upgrade to version 3.4 cannot be completed successfully if the host name of the KUMA Core begins with a numeral. If the hostname of the KUMA Core starts with a numeral, a number of steps are necessary to successfully complete the upgrade. Contact Technical Support for additional instructions.

4. During installation or upgrade, make sure KUMA storage hosts can access TCP port 7220 on the KUMA Core.

5. For event sources that have a red status in the **Source status** → **List of event sources** section, check out how many there are and if they are up to date; for outdated event sources, do one of the following:

   - Remove the event sources that you no longer need.

   - Edit the settings of monitoring policies that are applied to the outdated event sources to bring them up to date with the current stream of events.

   - For monitoring policies applied to outdated event sources, disable notifications.

   After KUMA is upgraded, notifications are sent to the configured email addresses for all red-status event sources that have notifications about triggered policies configured.

2 Updating KUMA

Depending on the KUMA deployment scheme that you are using, do one the following:

- Use the prepared `distributed.inventory.yml` inventory file and follow the instructions for distributed installation of the solution.

- Use the prepared `k0s.inventory.yml` inventory file and follow the instructions for distributed installation in a high availability configuration.

  If an inventory file is not available for the current version, use the provided inventory file template and edit it as necessary. To view a list of hosts and host roles in the current KUMA system, in the web interface, go to **Resources** → **Active services** section.

The upgrade process mirrors the installation process.

If you want to upgrade from a distributed installation to a distributed installation in a high availability configuration, first upgrade the distributed installation and then migrate the Core to a Kubernetes cluster.

How to transfer the KUMA Core to a Kubernetes cluster

To migrate KUMA Core to a new Kubernetes cluster:

1. Prepare the k0s.inventory.yml inventory file.

   The kuma_core, kuma_ collector, kuma_correlator, kuma_storage sections of your k0s.inventory.yml inventory file must contain the same hosts that were used when KUMA was upgraded from version 2.1.3 to version 3.0.3 and then to version 3.2, or when a new installation was performed. In the inventory file, set deploy_to_k8s: true, need_transfer: true. Set deploy_example_services: false.

2. Follow the steps for distributed installation using your prepared k0s.inventory.yml inventory file.

Migrating the KUMA Core to a new Kubernetes cluster

When the installer is started with an inventory file, the installer looks for an installed KUMA Core on all hosts where you plan to deploy worker nodes of the cluster. The found Core will be moved from the host to within the newly created Kubernetes cluster.

If the component is not detected on the worker nodes, a clean installation of the KUMA Core is performed in the cluster without migrating resources to it. Existing components must be manually rebuilt with the new Core in the KUMA web interface.

Certificates for collectors, correlators and storages will be re-issued from the inventory file for communication with the Core within the cluster. This does not change the Core URL for components.

On the Core host, the installer does the following:

- Removes systemd services from the host: kuma-core, kuma-vmalert.

- Deletes the internal certificate of the Core.

- Deletes the certificate files of all other components and deletes their records from MongoDB.

- Deletes the following directories:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/`<KUMA Core service ID>`/log
  - /opt/kaspersky/kuma/core/`<KUMA Core service ID>`/logs
  - /opt/kaspersky/kuma/metrics/`<Metrics service ID>`/bin
- Migrates data from the Core and its dependencies to a network drive within the Kubernetes cluster.
- On the Core host, it moves the following directories:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

After you have verified that the Core was correctly migrated to the cluster, you can delete these directories.

If you encounter problems with the migration, check the logs for records of the 'core-transfer' migration task in the 'kuma' namespace in the cluster (this task is available for 1 hour after the migration).

If you need to perform migration again, you must restore the original names of the /opt/kaspersky/kuma/*.moved directories.

If the /etc/hosts file on the Core host contained lines that were not related to addresses in the 127.X.X.X range, the contents of the /etc/hosts file from the Core host is entered into the coredns ConfigMap when the Core is migrated to the Kubernetes cluster. If the Core is not migrated, the contents of the /etc/hosts file from the host where the primary controller is deployed are entered into the ConfigMap.

For subsequent upgrades, use the `k0s.inventory.yml` inventory file with `need_transfer: false`, because the KUMA Core already has been migrated to the Kubernetes cluster and you do not need to repeat this.

3 Preparing KUMA for operation

1. After updating KUMA, you must clear your browser cache.
2. If you are using agents, manually update the KUMA agents.

The KUMA solution has been successfully upgraded.

Upgrading from version 3.4.x to 4.0

Limitations:

1. For existing users, upgrading from 3.4.x to 4.0 does not update the universal dashboard.

   Possible solution: restart the Core service, `kuma-core.service`. After a restart, the data is updated at the interval specified for the dashboard.

2. If the old Core service, `kuma-core.service` is still displayed after the upgrade, run the following command after installation is complete:

   ```
   sudo systemctl reset-failed
   ```

   After running the command, the old service is no longer displayed, and the new service starts successfully.

Upgrading KUMA from version 3.4.x to version 4.0 involves the following steps:

4 Preliminary steps

1. Make sure that all hardware and software requirements for solution installation are met.

2. Creating a backup copy of the KUMA Core. If necessary, you will be able to restore data from backup for version 3.4.x.

   KUMA backups created in versions 3.4.x and earlier cannot be restored in version 4.0. This means that you cannot install KUMA 4.0 and restore a KUMA 3.4.x backup in it.

   Create a backup copy immediately after upgrading KUMA to version 4.0.

3. Check the host name of the KUMA Core.

   The host name can begin with a numeral if this is consistent with the naming scheme adopted at the organization. However, for KUMA services to work with Raft, a host name may not start with a numeral.

   If your host name starts with a numeral, you do not need to rename the server. Configure an additional name (FQDN) that starts with a letter by following these steps:

   a. In the `/etc/hosts` file, add a line:

      ```
      <IP_address> <new_fqdn> <fqdn> <hostname>
      ```

      where:

      `<IP_address>` is the IP address of the server

      `<new_fqdn>` is the additional host name

      `<fqdn>` is the source FQDN.

      `<hostname>` is a short host name.

   b. On your DNS server, create a CNAME record in which `<new_fqdn>` points to `<fqdn>`.

   Use the configured alternate name for the KUMA services with Raft. You do not need to change the original host name.

4. During installation or update, ensure network accessibility of TCP port 7220 on the KUMA Core for the KUMA storage hosts.

5. For event sources that have a red status in the **Source status → List of event sources** section, check out how many there are and if they are up to date; for outdated event sources, do one of the following:

   - Remove the event sources that you no longer need.
   - Edit the settings of monitoring policies that are applied to the outdated event sources to bring them up to date with the current stream of events.
   - For monitoring policies applied to outdated event sources, disable notifications.

   After KUMA is upgraded, notifications are sent to the configured email addresses for all red-status event sources that have notifications about triggered policies configured.

6. For an installation with the KUMA Core in a Kubernetes cluster, determine the size of metrics data on the KUMA Core 3.4 volume to evaluate if you need to modify the values of the `metrics_transfer_job_timeout`, `metrics_disk_request`, `core_disk_request` settings in the `k0s.inventory.yml` inventory file; then proceed with the upgrade procedure.

   How to determine the size of metrics data on a KUMA Core 3.4 volume

   Run the get_old_metrics_size.sh script with the k0s.inventory.yml inventory file on the target machine using the following command:

   ```
   sudo ./get_old_metrics_size_sh k0s.inventory.yml
   ```

   This script does not make any changes to the existing installation. It connects to the primary controller of the cluster to determine the name of the KUMA Core volume and to the worker nodes of the cluster to determine the directory size inside the mounted volume.

   As a result, KUMA Core volumes are found on the worker nodes of the cluster, and the size of the `victoria-metrics` directory in them is determined. The output of the script is displayed and written to the `log/get_old_metrics_size-YYYYMMDD-HHMMSS.log` file.

   The following message is logged:

   ```
   TASK [Print metrics folder size] ************************************************
   ok: [kuma1.example.com] => {}

   MSG:

   Found KUMA Core 3.4.1.53
   Found old metrics folder size: 1Gi
   Minimum metrics_data_size required to proceed: 3Gi (including 2Gi threshold)
   ```

   where:

   - Found KUMA Core is the found version of the KUMA Core.
   - Found old metrics folder size is the current size of the `victoria-metrics` directory in gigabytes.
   - Minimum metrics_data_size required to proceed is the minimum possible size of the metrics volume for migration from version 3.4.x. This size includes a safety margin of 2Gi of free space. If necessary, you can filter the output by the `Minimum metrics_data_size required to proceed` string.

   Based on the results, you need to determine the required size of the Metrics service volume in KUMA 4.0.x, depending on your needs. The Metrics service volume size must not be less than the `Minimum metrics_data_size required to proceed` value.

When upgrading from version 3.4.x to version 4.0.x, if you specify a volume size less than the `Minimum metrics_data_size required to proceed` value in the inventory file `k0s.inventory.yml`, or if you specify the `metrics_disk_request` value that is less than the `Minimum metrics_data_size required to proceed` value, the installer aborts the upgrade at the installation validation stage with the following message:

```
TASK [Check metrics volume size requirement] ***********************************
fatal: [kuma1.example.com]: FAILED! => {
    "changed": false
}

MSG:

Current metrics folder size: 20Gi
Metrics disk request when low_resources=false: 10Gi
Metrics disk request when low_resources=true: 10Gi

Error: Available metric data exceeds specified volume size.
The available metric data (20Gi + 2Gi threshold) is too large.

Solution: Increase the metrics volume size by updating the metrics_disk_request variable in your inventory
file.
```

In the above example, the user tried to set the volume size to 10Gi through the `metrics_disk_request` inventory variable, while the current size of metrics data on the disk is 20Gi. The intended volume size is less than the current data size with the 2Gi safety margin, therefore the upgrade from version 3.4.x cannot be performed. The installation is aborted at the validation step, and no changes are made to the current installation. You can safely choose a suitable volume size for metrics, override it in the inventory file, and retry the upgrade.

❺ Upgrading KUMA

Depending on the KUMA deployment scheme that you are using, do one the following:

- Use the prepared `distributed.inventory.yml` inventory file and follow the instructions for distributed installation of the solution.

- Use the prepared `k0s.inventory.yml` inventory file and follow the instructions for distributed installation in a high availability configuration with the KUMA Core in a Kubernetes cluster.

  If an inventory file is not available for the current version, use the provided inventory file template and fill in the corresponding settings. To view a list of hosts and host roles in your current KUMA system, in the web interface, go to **Resources** → **Active services** section.

The upgrade process mirrors the installation process.

You can change the installation type as follows:

- If you want to upgrade from a distributed installation to an installation with the KUMA Core in a Kubernetes cluster, first upgrade the distributed installation to the latest version and then migrate the Core to a Kubernetes cluster.

  How to transfer the KUMA Core to a Kubernetes cluster

To migrate KUMA Core to a new Kubernetes cluster:

1. Prepare the k0s.inventory.yml inventory file.

   The kuma_core, kuma_ collector, kuma_correlator, kuma_storage sections of your k0s.inventory.yml inventory file must contain the same hosts that were used when KUMA was upgraded from version 2.1.3 to version 3.0.3 and then to version 3.2, or when a new installation was performed. In the inventory file, set deploy_to_k8s: true, need_transfer: true. Set deploy_example_services: false.

2. Follow the steps for distributed installation using your prepared k0s.inventory.yml inventory file.

Migrating the KUMA Core to a new Kubernetes cluster

When the installer is started with an inventory file, the installer looks for an installed KUMA Core on all hosts where you plan to deploy worker nodes of the cluster. The found Core will be moved from the host to within the newly created Kubernetes cluster.

If the component is not detected on the worker nodes, a clean installation of the KUMA Core is performed in the cluster without migrating resources to it. Existing components must be manually rebuilt with the new Core in the KUMA web interface.

Certificates for collectors, correlators and storages will be re-issued from the inventory file for communication with the Core within the cluster. This does not change the Core URL for components.

On the Core host, the installer does the following:

- Removes systemd services from the host: kuma-core, kuma-vmalert.
- Deletes the internal certificate of the Core.
- Deletes the certificate files of all other components and deletes their records from MongoDB.
- Deletes the following directories:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/log
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/logs
  - /opt/kaspersky/kuma/metrics/<Metrics service ID>/bin
- Migrates data from the Core and its dependencies to a network drive within the Kubernetes cluster.
- On the Core host, it moves the following directories:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

After you have verified that the Core was correctly migrated to the cluster, you can delete these directories.

If you encounter problems with the migration, check the logs for records of the 'core-transfer' migration task in the 'kuma' namespace in the cluster (this task is available for 1 hour after the migration).

If you need to perform migration again, you must restore the original names of the /opt/kaspersky/kuma/*.moved directories.

If the /etc/hosts file on the Core host contained lines that were not related to addresses in the 127.X.X.X range, the contents of the /etc/hosts file from the Core host is entered into the coredns ConfigMap when the Core is migrated to the Kubernetes cluster. If the Core is not migrated, the contents of the /etc/hosts file from the host where the primary controller is deployed are entered into the ConfigMap.

For subsequent upgrades, use the `k0s.inventory.yml` inventory file with `need_transfer: false`, because the KUMA Core already has been migrated to the Kubernetes cluster and you do not need to repeat this.

- If you want to upgrade KUMA in a distributed installation to the latest version of KUMA with the Core in a Raft cluster, add a `kuma_core_peers` section to the `distributed.inventory.yml` inventory file and in this section, specify an even number of servers on which you plan to install additional KUMA Core services. Also, in the `kuma_core` and `kuma_core_peers` sections, you can specify the `raft_node_addr` setting in the <FQDN of the server from the kuma_core section on which the KUMA Core is installed>:<port> format, if the server has multiple FQDNs. The FQDN specified in the `raft_node_addr` setting will be used to listen for signals from other nodes.

  After starting the installer with the prepared inventory file, none of the additional KUMA Core services are automatically installed on the servers. The installer only prepares the servers specified in the inventory file for the installation of services. After the installer finishes, only one KUMA Core service is automatically installed on the server specified in the `kuma_core` section. After the installer finishes, you need to manually create the KUMA Core services in the web interface and install the KUMA Core services with unique IDs one by one on each server specified in the `kuma_core_peers` section.

  After the upgrade, all existing KUMA services are connected to the KUMA Core on the server from the `kuma_core` section. Subsequently, when installing new services, you can specify multiple comma-separated URLs in the installation command to connect services to KUMA Cores in the Raft cluster.

6 Preparing KUMA for operation

1. After updating KUMA, you must clear your browser cache.

2. If you are using agents, manually update the KUMA agents.

3. Migrate alert events from MongoDB to ClickHouse.

   How to migrate alert events

   After upgrading KUMA from version 3.4.x to version 4.0, you need to migrate alert events from MongoDB to ClickHouse and specify a storage in the alert filling settings.

   After upgrading KUMA, the installer stops the `kuma-mongodb` service, which you must start manually before migrating alert events. If the KUMA Core is deployed in a Kubernetes cluster, the MongoDB container is also not started after the upgrade, so you need to start it before the migration.

   If you need to abort the alert event migration command, press **`Ctrl+C`** in the terminal. A notification appears stating that the command will be stopped. The current batch of events is safely transferred to the storage, the migration progress is retained, and the process can be continued the next time you run the command.

Alert event migration is available for the following installation types:

- KUMA in a non-high-availability configuration
- In a high-availability configuration in a Kubernetes cluster

Migrating alert events after upgrading a non-high-availability KUMA installation

To migrate alert events in a non-high-availability configuration:

1. In the web interface, in the **Resources** → **Active services** section, select the storage to which you want to move the alert events and click **Copy cluster ID**.

   You will need the ID of the storage cluster when running the alert event migration command.

2. On the KUMA Core server, start `kuma-mongodb.service` using the following command:

   ```
   sudo systemctl start kuma-mongodb.service
   ```

3. Go to the `/opt/kaspersky/kuma` directory and run the following command, specifying the options as necessary and specifying the previously copied storage cluster ID in the `--cluster-id` option:

   ```
   ./kuma tools migrate --mongo="mongodb://<mongo_hostname>:<port>" --core-url="https://<FQDN>:<port>" --core-dir="<core_directory>" --cluster-id="<cluster_id>" --batch=<events_count> 2>&1 | tee /tmp/migrate.log | grep -v "debug"
   ```

   where:

   - <mongo_hostname> is the hostname of the host on which MongoDB is installed.
   - <FQDN> is the fully qualified domain name of the server on which KUMA Core is installed.
   - <port> is the port number of the KUMA Core server.
   - <core_directory> is the directory for storing KUMA Core data; depending on the type of installation, it is /opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000 or /opt/kaspersky/kuma/core.
   - <cluster_id> is the ID of the storage cluster to which want to migrate the KUMA 3.4 alert events.
   - <events_count> is the count of alert events in the batch.

   Example

   ```
   ./kuma tools migrate --mongo="mongodb://localhost:27017" --core-url="https://kuma.example.com:7210" --core-dir="/opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000" --cluster-id="0a123456-789a-0123-ab12-a3fab45ab6a7" --batch=10000 2>&1 | tee /tmp/migrate.log | grep -v "debug"
   ```

   Possible settings for alert event migration from MongoDB to ClickHouse

   The complete output of the command is saved to the `/tmp/migrate.log` file.

Migration can take a long time if there are many alerts. To speed up the migration process, you can use the `--batch` option and pre-allocate additional disk space and RAM. For example, you can migrate 150,000 alerts in one iteration lasting approximately three minutes with 12 GB of RAM for the migrator and MongoDB and 30 GB of disk space with the `--batch` option set to `150000`. In this example, the values and the duration of alert event migration are given as a rough estimate. The duration may differ depending on the number of alerts and the number of events in alerts, the available disk space and RAM, and the number of alert events per batch specified in the `--batch` option. You can adapt these values to your needs.

You can also speed up the migration if you want to migrate only some alert events, for example, only alert events for the last year. In this case, you can specify the `--time-limit`, which corresponds to the **Alert retention period, days** setting.

For example, you have alert events for the past year and a half, and you want to migrate alert events for the last year. If you initiate the migration on August 18, 2025, and the **Alert retention period, days** is set to **365**, then set the `--time-limit` option to August 19, 2024 as follows: `--time-limit="Sun, 19 Aug 2024 00:01:00 UTC"`.

Only alert events for the last 365 days are migrated. This speeds up the migration of alert events and avoids moving unwanted events.

If you do not specify the `--time-limit`, all alert events are migrated to ClickHouse, but this may take more time, and alert events older than the specified alert retention period will be subsequently deleted from ClickHouse.

4. After running the command, stop the `mongodb` service and disable it with the following commands:

```
sudo systemctl stop kuma-mongodb.service
```

```
sudo systemctl disable kuma-mongodb.service
```

Alert events are migrated.

After completing the KUMA upgrade and migrating alert events, the storage for new alert events is not automatically specified. The storage cluster you have specified is only for the migration of existing alert events. For new alerts to be filled with events, you must manually specify the **Storage** in the alert filling settings. Until you specify this setting, new alerts will be generated without events.

Migrating alert events after upgrading an installation with KUMA Core in a Kubernetes cluster

To migrate alert events in a KUMA installation with KUMA Core in a Kubernetes cluster:

1. In the web interface, in the **Resources** → **Active services** section, select the storage to which you want to move the alert events and click **Copy ID**. You will need the ID of the storage cluster when running the alert event migration command.

2. Start the MongoDB container in the KUMA Core pod by running the following command on the master controller:

```
sudo k0s kubectl apply -f /root/k0s/core-manifest.yaml
```

The KUMA Core is restarted.

3. Connect to the master controller of the `k0s` cluster and start the migration of alert events by substituting the previously obtained storage cluster identifier in the `--cluster-id` option:

```
k0s kubectl exec -it deployment/core-deployment -c core -n kuma -- kuma tools migrate --
mongo="mongodb://127.0.0.1:27017" --core-url="https://core:7210" --core-dir="/opt/kaspersky/kuma/core" --
cluster-id="ec9e34bc-8c05-4f95-bb37-cfd5fe4b354a" --wd="/opt/kaspersky/kuma/core" --batch=10000 2>&1 | tee
/tmp/migrate.log | grep -v "debug"
```

Possible settings for alert event migration from MongoDB to ClickHouse

The complete output of the command is saved to the `/tmp/migrate.log` file on the host where you run `k0s kubectl`, not on the volume of the pod.

Migration can take a long time if there are many alerts. If the SSH session is interrupted, the command continues to run on the pod. In this case, you do not need to run the command again. You can watch the execution of the command in the processes on the worker node where the KUMA Core is running:

```
sudo watch 'ps -faux | grep "kuma tools migrate"'
```

To speed up the migration process, you can use the `--batch` option and pre-allocate additional disk space and RAM. For example, you can migrate 150,000 alerts in one iteration lasting approximately three minutes with 12 GB of RAM for the migrator and MongoDB and 30 GB of disk space with the `--batch` option set to 150000. In this example, the values and the duration of alert event migration are given as a rough estimate. The duration may differ depending on the number of alerts and the number of events in alerts, the available disk space and RAM, and the number of alert events per batch specified in the `--batch` option. You can adapt these values to your needs.

You can also speed up the migration if you want to migrate only some alert events, for example, only alert events for the last year. In this case, you can specify the `--time-limit`, which corresponds to the **Alert retention period, days** setting.

For example, you have alert events for the past year and a half, and you want to migrate alert events for the last year. If you initiate the migration on August 18, 2025, and the **Alert retention period, days** is set to **365**, then set the `--time-limit` option to August 19, 2024 as follows:

```
--time-limit="Sun, 19 Aug 2024 00:01:00 UTC"
```

Only alert events for the last 365 days are migrated. This speeds up the migration of alert events and avoids moving unwanted events.

If you do not specify the `--time-limit`, all alert events are migrated to ClickHouse, but this may take more time, and alert events older than the specified alert retention period will be subsequently deleted from ClickHouse.

4. After successfully migrating alert events, we recommend starting the KUMA Core without the MongoDB container. To do this, on the master controller, run the KUMA Core without the MongoDB container using the following command:

```
sudo k0s kubectl apply -f /root/k0s/core-manifest-no-mongodb.yaml
```

The KUMA Core is restarted.

Alert events are migrated.

After completing the KUMA upgrade and migrating alert events, the storage for new alert events is not automatically specified. The storage cluster you have specified is only for the migration of existing alert

events. For new alerts to be filled with events, you must manually specify the **Storage** in the alert filling settings. Until you specify this setting, new alerts will be generated without events.

After migrating alert events to KUMA, you need to take into account the special considerations involved in their backup and restoration processes using the REST API.

4. Specify the storage for new alert events in alert filling settings.

The KUMA solution has been successfully upgraded.

Upgrading from version 4.0.x to 4.2

Limitations:

- For existing users, upgrading from 4.0.x to 4.2 does not update the universal dashboard.

  Possible solution: restart the `kuma-core-<KUMA Core service ID>.service` service. After a restart, the data is updated at the interval specified for the dashboard.

Upgrading KUMA from version 4.0.x to version 4.2 involves the following steps:

7 Preliminary steps

1. Make sure that all hardware and software requirements for solution installation are met.

2. Creating a backup copy of the KUMA Core. If necessary, you will be able to restore data from backup for version 4.0.x.

   KUMA backups created in versions 4.0.x and earlier cannot be restored in version 4.2 This means that you cannot install KUMA 4.2 and restore a KUMA 4.0.x backup in it.

   Create a backup copy immediately after upgrading KUMA to version 4.2.

3. Check the host name of the KUMA Core.

   The host name can begin with a numeral if this is consistent with the naming scheme adopted at the organization. However, for KUMA services to work with Raft, a host name may not start with a numeral.

   If your host name starts with a numeral, you do not need to rename the server. Configure an additional name (FQDN) that starts with a letter by following these steps:

   a. In the `/etc/hosts` file, add a line:

   ```
   <IP_address> <new_fqdn> <fqdn> <hostname>
   ```

   where:

   `<IP_address>` is the IP address of the server

   `<new_fqdn>` is the additional host name

   `<fqdn>` is the source FQDN.

   `<hostname>` is a short host name.

   b. On your DNS server, create a CNAME record in which `<new_fqdn>` points to `<fqdn>`.

Use the configured alternate name for the KUMA services with Raft. You do not need to change the original host name.

4. During installation or update, ensure network accessibility of TCP port 7220 on the KUMA Core for the KUMA storage hosts.

5. For event sources that have a red status in the **Source status** → **List of event sources** section, check out how many there are and if they are up to date; for outdated event sources, do one of the following:

   - Remove the event sources that you no longer need.

   - Edit the settings of monitoring policies that are applied to the outdated event sources to bring them up to date with the current stream of events.

   - For monitoring policies applied to outdated event sources, disable notifications.

   After KUMA is upgraded, notifications are sent to the configured email addresses for all red-status event sources that have notifications about triggered policies configured.

8 Updating KUMA

Depending on the KUMA deployment scheme that you are using, do one the following:

- Use the prepared `distributed.inventory.yml` inventory file and follow the instructions for distributed installation of the solution. In the inventory file, in the `kuma_metrics` section, you need to specify the host on which the active Metrics service is running. When the update starts, a check is performed, and if the Metrics service is not found on the specified host, an error is returned and the update is stopped.

- Use the prepared `k0s.inventory.yml` inventory file and follow the instructions for distributed installation in a high availability configuration with the KUMA Core in a Kubernetes cluster.

  In the inventory file, in the `kuma_metrics` section, you need to specify the host on which the active Metrics service is running. When the update starts, a check is performed, and if the Metrics service is not found on the specified host, an error is returned and the update is stopped.

  If an inventory file is not available for the current version, use the provided inventory file template and fill in the corresponding settings. To view a list of hosts and host roles in the current KUMA system, in the web interface, go to **Resources** → **Active services** section.

The upgrade process mirrors the installation process.

You can change the installation type as follows:

- If you want to upgrade from a distributed installation to an installation with the KUMA Core in a Kubernetes cluster, first upgrade the distributed installation to the latest version and then migrate the Core to a Kubernetes cluster.

  How to transfer the KUMA Core to a Kubernetes cluster

To migrate KUMA Core to a new Kubernetes cluster:

1. Prepare the k0s.inventory.yml inventory file.

   The kuma_core, kuma_ collector, kuma_correlator, kuma_storage sections of your k0s.inventory.yml inventory file must contain the same hosts that were used when KUMA was upgraded from version 2.1.3 to version 3.0.3 and then to version 3.2, or when a new installation was performed. In the inventory file, set deploy_to_k8s: true, need_transfer: true. Set deploy_example_services: false.

2. Follow the steps for distributed installation using your prepared k0s.inventory.yml inventory file.

Migrating the KUMA Core to a new Kubernetes cluster

When the installer is started with an inventory file, the installer looks for an installed KUMA Core on all hosts where you plan to deploy worker nodes of the cluster. The found Core will be moved from the host to within the newly created Kubernetes cluster.

If the component is not detected on the worker nodes, a clean installation of the KUMA Core is performed in the cluster without migrating resources to it. Existing components must be manually rebuilt with the new Core in the KUMA web interface.

Certificates for collectors, correlators and storages will be re-issued from the inventory file for communication with the Core within the cluster. This does not change the Core URL for components.

On the Core host, the installer does the following:

- Removes systemd services from the host: kuma-core, kuma-vmalert.
- Deletes the internal certificate of the Core.
- Deletes the certificate files of all other components and deletes their records from MongoDB.
- Deletes the following directories:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/log
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/logs
  - /opt/kaspersky/kuma/metrics/<Metrics service ID>/bin
- Migrates data from the Core and its dependencies to a network drive within the Kubernetes cluster.
- On the Core host, it moves the following directories:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

After you have verified that the Core was correctly migrated to the cluster, you can delete these directories.

If you encounter problems with the migration, check the logs for records of the 'core-transfer' migration task in the 'kuma' namespace in the cluster (this task is available for 1 hour after the migration).

If you need to perform migration again, you must restore the original names of the /opt/kaspersky/kuma/*.moved directories.

If the /etc/hosts file on the Core host contained lines that were not related to addresses in the 127.X.X.X range, the contents of the /etc/hosts file from the Core host is entered into the coredns ConfigMap when the Core is migrated to the Kubernetes cluster. If the Core is not migrated, the contents of the /etc/hosts file from the host where the primary controller is deployed are entered into the ConfigMap.

For subsequent upgrades, use the `k0s.inventory.yml` inventory file with `need_transfer: false`, because the KUMA Core already has been migrated to the Kubernetes cluster and you do not need to repeat this.

- If you want to upgrade KUMA in a distributed installation to the latest version of KUMA with the Core in a Raft cluster, add a `kuma_core_peers` section to the `distributed.inventory.yml` inventory file and in this section, specify an even number of servers on which you plan to install additional KUMA Core services. Also, in the `kuma_core` and `kuma_core_peers` sections, you can specify the `raft_node_addr` setting in the <FQDN of the server from the kuma_core section on which the KUMA Core is installed>:<port> format, if the server has multiple FQDNs. The FQDN specified in the `raft_node_addr` setting will be used to listen for signals from other nodes.

  After starting the installer with the prepared inventory file, none of the additional KUMA Core services are automatically installed on the servers. The installer only prepares the servers specified in the inventory file for the installation of services. After the installer finishes, only one KUMA Core service is automatically installed on the server specified in the `kuma_core` section. After the installer finishes, you need to manually create the KUMA Core services in the web interface and install the KUMA Core services with unique IDs one by one on each server specified in the `kuma_core_peers` section.

  After the upgrade, all existing KUMA services are connected to the KUMA Core on the server from the `kuma_core` section. Subsequently, when installing new services, you can specify multiple comma-separated URLs in the installation command to connect services to KUMA Cores in the Raft cluster.

9 Preparing KUMA for operation

1. After updating KUMA, you must clear your browser cache.

2. If you are using agents, manually update the KUMA agents.

3. For a distributed installation in a high-availability configuration with KUMA Core in a Kubernetes cluster, upgrade the cluster components.

   How to upgrade Kubernetes cluster components

   Kubernetes cluster components need to be upgraded only if KUMA is being upgraded to version 4.2.x. When installing KUMA 4.2.x from scratch, a Kubernetes cluster component upgrade is not necessary.

   > Before upgrading your Kubernetes cluster components, you need to manually back up the KUMA Core 4.2 in case of unforeseen issues with the upgrade. If you do not have a manually created backup copy of the KUMA Core 4.2, all data may be lost in the event of a failure.

   Kubernetes cluster components must be upgraded from a dedicated ansible-controller machine that is not a member of the Kubernetes cluster because the upgrade script restarts all cluster hosts. If a machine inside the cluster is used as the ansible-controller, the restart of the cluster hosts stops the execution of the script and the cluster becomes inoperable.

Kubernetes cluster components are upgraded using the `cluster_upgrade.sh` script and the `k0s.inventory.yaml` inventory file, only on hosts from the `k0s` section of the `k0s.inventory.yaml` inventory file. External KUMA services are not affected.

By default, the upgrade script automatically creates a backup copy.

If creating a manual backup of the KUMA Core, as recommended for unforeseen contingencies, took a long time and you do not want to wait a similar amount of time for the automatic backup to be created, you can place your manual backup on the dedicated ansible-controller machine in a `autobackup.tar.gz` file and run the script with the `-e 'manual_restore_only=true'` option. The `-e 'manual_restore_only=true'` option skips the automatic backup and restore, speeding up the upgrade. In this case, you will need to restore the KUMA Core from a backup copy manually.

The following methods are available for upgrading Kubernetes cluster components:

Upgrading Kubernetes cluster components without the -e 'manual_restore_only=true' option

To upgrade Kubernetes cluster components without the -e 'manual_restore_only=true' option:

1. Prepare for the upgrade:

   a. Make sure that KUMA has been upgraded from version 4.0.x to 4.2.x using the install.sh installer and the `k0s.inventory.yaml` inventory file.

   b. Prepare the dedicated ansible-controller machine from which you are going to run the update script, and make sure that this machine does not belong to the cluster. The update script restarts all hosts in the cluster. If the ansible-controller machine belongs to the cluster, the restart of the cluster hosts stops the script, and the installation of new versions of Kubernetes components fails, leaving the cluster inoperable.

   c. Make sure there is enough free disk space on the dedicated ansible-controller machine and on the master-controller to accommodate the backup data.

   d. Manually create a backup copy of the KUMA Core to prepare for unforeseen issues.

      The metrics data is not included in the backup copy and is not migrated to the Kubernetes cluster. When you upgrade the components of the Kubernetes cluster, the metrics data will be lost.

      If the metrics data is critically important to you, contact Technical Support before upgrading the Kubernetes cluster components.

   e. Specify the `backup_timeout` setting value in the `k0s.inventory.yaml` inventory file in the `vars` section.

2. Perform the upgrade:

   a. On the dedicated ansible-controller machine, go to the directory of the 4.2 version installer and run the cluster_upgrade.sh script, passing the name of the current inventory file k0s.inventory.yaml as an argument:

      ```
      ./cluster_upgrade.sh k0s.inventory.yaml
      ```

   b. On the command line, confirm that you have a backup copy of the KUMA Core and agree to the upgrade by entering `yes`.

During the upgrade process, the KUMA Core is automatically backed up in the `autobackup.tar.gz` archive. The script creates a backup copy of the KUMA Core on the master-controller machine in the `/root/k0s` directory, and then transfers it to the directory with the script on the dedicated ansible-controller machine from which you are upgrading the Kubernetes components. The automatic recovery of KUMA Core data in the new Kubernetes cluster also involves the installer directory and the `/root/k0s` directory on the master-controller machine.

Later, the KUMA Core will be automatically restored from the backup copy in the new Kubernetes cluster. If the upgrade fails, you can place your manually created backup copy into the `autobackup.tar.gz` file in the script directory on the ansible-controller machine and run the `cluster_upgrade.sh` script again.

The created backup copy is not automatically overwritten.

The Kubernetes cluster components are upgraded.

Failure recovery

The following scenarios are available for failure recovery:

- Failure to upgrade Kubernetes cluster components. You can use any of the following recovery options:
  - Place your manually created backup copy into the `autobackup.tar.gz` file in the script directory on the master-controller machine and run the `cluster_upgrade.sh` script again. The script processes the manually created backup copy and continues the upgrade procedure.
  - Run the `cluster_upgrade.sh` script with the `-e 'manual_restore_only=true'` option and perform the recovery manually.
- Failure to start the KUMA Core after a successful upgrade of the Kubernetes cluster.

  If you want the script to automatically repeat the uninstallation and new installation of the cluster, you must stop the k0s service on any of the cluster nodes and delete the k0s executable file on that node. As a result, the script will interpret the state of the cluster as inconsistent and will uninstall and reinstall the cluster using the previously created `autobackup.tar.gz` file.

  To stop the k0s service on cluster controllers and hosts that combine the roles of a controller and a worker node, run the following commands:

  ```
  sudo systemctl stop k0scontroller.service
  sudo rm /usr/bin/k0s
  ```

  To stop the k0s service and delete the k0s binary file on dedicated worker nodes, run the following commands:

  ```
  sudo systemctl stop k0sworker.service
  sudo rm /usr/bin/k0s
  ```

  The cluster is uninstalled only after obtaining a correct backup file or explicitly refusing to use the automatic backup and restoration by passing the `-e 'manual_restore_only=true'` option and agreeing to proceed with the upgrade without performing a backup. If you do not have a manually created backup copy of the, all data will be lost in the event of a failure.

Upgrading Kubernetes cluster components with the -e 'manual_restore_only=true' option

To upgrade Kubernetes cluster components with the -e 'manual_restore_only=true' option

1. Prepare for the upgrade:

   a. Make sure that KUMA has been upgraded from version 4.0.x to 4.2.x using the `install.sh` installer and the `k0s.inventory.yaml` inventory file.

   b. Prepare the dedicated ansible-controller machine from which you are going to run the update script, and make sure that this machine does not belong to the cluster. The update script restarts all hosts in the cluster. If the ansible-controller machine belongs to the cluster, the restart of the cluster hosts stops the script, and the installation of new versions of Kubernetes components fails, leaving the cluster inoperable.

   c. Make sure there is enough free disk space on the dedicated ansible-controller machine and on the master-controller to accommodate the backup data.

   d. Manually create a backup copy of the KUMA Core to prepare for unforeseen issues.

      The metrics data is not included in the backup copy and is not migrated to the Kubernetes cluster. When you upgrade the components of the Kubernetes cluster, the metrics data will be lost.

      If the metrics data is critically important to you, contact Technical Support before upgrading the Kubernetes cluster components.

2. Perform the upgrade:

   a. On the dedicated ansible-controller machine, go to the directory of the KUMA 4.2 installer and run the cluster_upgrade.sh script, passing the name of the current inventory file k0s.inventory.yaml and the `-e 'manual_restore_only=true'` option:

      ```
      ./cluster_upgrade.sh k0s.inventory.yaml [-e 'manual_restore_only=true']
      ```

      Automatic backup and restoration is disabled. The script uninstalls the old cluster and creates a new Kubernetes cluster.

   b. On the command line, confirm that you have a backup copy of the KUMA Core and agree to the upgrade by entering `yes`.

      If you do not have a manually created backup copy, confirming the uninstallation of the cluster causes the data to be lost.

3. Restore the KUMA Core from backup.

The Kubernetes cluster components are upgraded.

Failure recovery

If the upgrade fails, run the `cluster_upgrade.sh` script again and manually restore the KUMA Core from the backup copy.

The KUMA solution has been successfully upgraded.

Upgrading from version 4.2 to 4.6

Limitations:

- For existing users, upgrading from version 4.2 to 4.6 does not update the universal dashboard layout.

  Possible solution: restart the `kuma-core-<KUMA Core service ID>.service` service. After a restart, the data is updated at the interval specified for the dashboard.

Upgrading KUMA from version 4.2 to version 4.6 involves the following steps:

⑩ Preliminary steps

1. Make sure that all hardware and software requirements for solution installation are met.

   > The minimum compatible version of the Linux kernel on the target hosts is 5.15

2. If the KUMA solution is deployed in a Kubernetes cluster, and you upgrade KUMA in the following sequence: 4.0 → 4.2 → 4.6, you need to reissue the certificates of the KUMA metrics service. To do this, in KUMA 4.2, after upgrading the components of the Kubernetes cluster:

   a. Delete the certificates of the metrics service. To do this, on any controller of the Kubernetes cluster, run the following commands as root:

   ```
   k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
   k0s kubectl rollout restart deployment metrics -n kuma
   ```

   b. Reset the certificates of the metrics service in the **Active services** section. After that, make sure that the metrics service is displayed with a green status.

3. Creating a backup copy of the KUMA Core. If necessary, you will be able to restore data from backup for version 4.2.

   KUMA backups created in versions 4.2 and earlier cannot be restored in version 4.6. This means that you cannot install KUMA 4.6 and restore a KUMA 4.2 backup in it.

   Create a backup copy immediately after upgrading KUMA to version 4.6.

4. Check the host name of the KUMA Core.

   The host name can begin with a numeral if this is consistent with the naming scheme adopted at the organization. However, for KUMA services to work with Raft, a host name may not start with a numeral.

   If your host name starts with a numeral, you do not need to rename the server. Configure an additional name (FQDN) that starts with a letter by following these steps:

   a. In the `/etc/hosts` file, add a line:

   ```
   <IP_address> <new_fqdn> <fqdn> <hostname>
   ```

   where:

   `<IP_address>` is the IP address of the server

   `<new_fqdn>` is the additional host name

   `<fqdn>` is the source FQDN.

`<hostname>` is a short host name.

b. On your DNS server, create a CNAME record in which `<new_fqdn>` points to `<fqdn>`.

Use the configured alternate name for the KUMA services with Raft. You do not need to change the original host name.

5. During installation or update, ensure network accessibility of TCP port 7220 on the KUMA Core for the KUMA storage hosts.

6. For event sources that have a red status in the **Source status** → **List of event sources** section, check out how many there are and if they are up to date; for outdated event sources, do one of the following:

   - Remove the event sources that you no longer need.
   - Edit the settings of monitoring policies that are applied to the outdated event sources to bring them up to date with the current stream of events.
   - For monitoring policies applied to outdated event sources, disable notifications.

   After KUMA is upgraded, notifications are sent to the configured email addresses for all red-status event sources that have notifications about triggered policies configured.

11 Updating KUMA

Depending on the KUMA deployment scheme that you are using, do one the following:

- Use the prepared `distributed.inventory.yml` inventory file and follow the instructions for distributed installation of the solution. In the inventory file, in the `kuma_metrics` section, you need to specify the host on which the active Metrics service is running. When the update starts, a check is performed, and if the Metrics service is not found on the specified host, an error is returned and the update is stopped.

- Use the prepared `k0s.inventory.yml` inventory file and follow the instructions for distributed installation in a high availability configuration with the KUMA Core in a Kubernetes cluster. Make sure you are using Kubernetes version 1.33.

  In the inventory file, in the `kuma_metrics` section, you need to specify the host on which the active Metrics service is running. When the update starts, a check is performed, and if the Metrics service is not found on the specified host, an error is returned and the update is stopped.

  If an inventory file is not available for the current version, use the provided inventory file template and fill in the corresponding settings. To view a list of hosts and host roles in the current KUMA system, in the web interface, go to **Resources** → **Active services** section.

The upgrade process mirrors the installation process.

You can change the installation type as follows:

- If you want to upgrade from a distributed installation to an installation with the KUMA Core in a Kubernetes cluster, first upgrade the distributed installation to the latest version and then migrate the Core to a Kubernetes cluster.

  How to transfer the KUMA Core to a Kubernetes cluster

To migrate KUMA Core to a new Kubernetes cluster:

1. Prepare the k0s.inventory.yml inventory file.

   The kuma_core, kuma_ collector, kuma_correlator, kuma_storage sections of your k0s.inventory.yml inventory file must contain the same hosts that were used when KUMA was upgraded from version 2.1.3 to version 3.0.3 and then to version 3.2, or when a new installation was performed. In the inventory file, set deploy_to_k8s: true, need_transfer: true. Set deploy_example_services: false.

2. Follow the steps for distributed installation using your prepared k0s.inventory.yml inventory file.

Migrating the KUMA Core to a new Kubernetes cluster

When the installer is started with an inventory file, the installer looks for an installed KUMA Core on all hosts where you plan to deploy worker nodes of the cluster. The found Core will be moved from the host to within the newly created Kubernetes cluster.

If the component is not detected on the worker nodes, a clean installation of the KUMA Core is performed in the cluster without migrating resources to it. Existing components must be manually rebuilt with the new Core in the KUMA web interface.

Certificates for collectors, correlators and storages will be re-issued from the inventory file for communication with the Core within the cluster. This does not change the Core URL for components.

On the Core host, the installer does the following:

- Removes systemd services from the host: kuma-core, kuma-vmalert.
- Deletes the internal certificate of the Core.
- Deletes the certificate files of all other components and deletes their records from MongoDB.
- Deletes the following directories:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/log
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/logs
  - /opt/kaspersky/kuma/metrics/<Metrics service ID>/bin
- Migrates data from the Core and its dependencies to a network drive within the Kubernetes cluster.
- On the Core host, it moves the following directories:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

After you have verified that the Core was correctly migrated to the cluster, you can delete these directories.

If you encounter problems with the migration, check the logs for records of the 'core-transfer' migration task in the 'kuma' namespace in the cluster (this task is available for 1 hour after the migration).

If you need to perform migration again, you must restore the original names of the /opt/kaspersky/kuma/*.moved directories.

If the /etc/hosts file on the Core host contained lines that were not related to addresses in the 127.X.X.X range, the contents of the /etc/hosts file from the Core host is entered into the coredns ConfigMap when the Core is migrated to the Kubernetes cluster. If the Core is not migrated, the contents of the /etc/hosts file from the host where the primary controller is deployed are entered into the ConfigMap.

For subsequent upgrades, use the `k0s.inventory.yml` inventory file with `need_transfer: false`, because the KUMA Core already has been migrated to the Kubernetes cluster and you do not need to repeat this.

- If you want to upgrade KUMA in a distributed installation to the latest version of KUMA with the Core in a Raft cluster, add a `kuma_core_peers` section to the `distributed.inventory.yml` inventory file and in this section, specify an even number of servers on which you plan to install additional KUMA Core services. Also, in the `kuma_core` and `kuma_core_peers` sections, you can specify the `raft_node_addr` setting in the <FQDN of the server from the kuma_core section on which the KUMA Core is installed>:<port> format, if the server has multiple FQDNs. The FQDN specified in the `raft_node_addr` setting will be used to listen for signals from other nodes.

  After starting the installer with the prepared inventory file, none of the additional KUMA Core services are automatically installed on the servers. The installer only prepares the servers specified in the inventory file for the installation of services. After the installer finishes, only one KUMA Core service is automatically installed on the server specified in the `kuma_core` section. After the installer finishes, you need to manually create the KUMA Core services in the web interface and install the KUMA Core services with unique IDs one by one on each server specified in the `kuma_core_peers` section.

  After the upgrade, all existing KUMA services are connected to the KUMA Core on the server from the `kuma_core` section. Subsequently, when installing new services, you can specify multiple comma-separated URLs in the installation command to connect services to KUMA Cores in the Raft cluster.

⓬ Preparing KUMA for operation

1. After updating KUMA, you must clear your browser cache.

2. If you are using agents, manually update the KUMA agents.

3. In KUMA Core settings, in the **KUMA resources localization** drop-down list, select a localization language for KUMA resources imported from the repository. The default language is English.

The KUMA solution has been successfully upgraded.

Useful articles

Kaspersky Unified Monitoring and Analysis Platform upgrade errors

Upgrading Oracle Linux 8.x to Oracle Linux 9.x with installed KUMA services

To upgrade Oracle Linux 8.x to Oracle Linux 9.x:

1. Run the following commands to disable KUMA services on the hosts where the services are installed:

```
sudo systemctl disable kuma-collector-<service ID>.service
sudo systemctl disable kuma-correlator-<service ID>.service
sudo systemctl disable kuma-storage-<service ID>.service
sudo systemctl disable kuma-metrics-<metrics service ID>.service
sudo systemctl disable kuma-vmalert.service
sudo systemctl disable kuma-core-<KUMA Core service ID>.service
```

2. Upgrade the operating system on each host.

3. Run the following commands to enable the services on the hosts where the services are installed:

```
sudo systemctl enable kuma-core-<KUMA Core service ID>.service
sudo systemctl enable kuma-storage-<service ID>.service
sudo systemctl enable kuma-collector-<service ID>.service
sudo systemctl enable kuma-correlator-<service ID>.service
sudo systemctl enable kuma-metrics-<metrics service ID>.service
sudo systemctl enable kuma-vmalert.service
```

4. Restart the hosts.

The upgrade is completed.

Data back up and recovery

A full backup allows KUMA Core to be restored after critical failures, update errors, migration between KUMA instances, or data loss.

A backup copy contains all the entities required to return the system to an operational state:

- alerts;
- assets and accounts;
- resources (collectors, normalizers, rules, dictionaries, and other configuration objects);
- parameters of integration with external systems.

To migrate or copy resources, use the resource export and import functionality instead. Resource export allows individual configuration objects to be restored without restoring the entire infrastructure. This reduces recovery time after erroneous changes and decreases the risk of losing current configurations of rules, normalizers, and dictionaries.

To ensure that the backups are up-to-date, we recommend doing the following:

1. Create a full backup of KUMA Core at least once every seven days.
2. Export resources every 24 hours.
3. Store several generations of backups and monitor the success of their creation.

The following backup and restore methods are available:

- Using the REST API
- In the web interface

You can also create backups of individual partitions on a schedule or manually.

Special considerations for KUMA backup

- Data may only be restored from a backup if it is restored to the KUMA of the same version as the backup one.

  > If you perform a backup in KUMA 4.0 or later, and then restore the backup to another device with KUMA 4.0 or later using the REST API (`system/backup → system/restore`), alert events are not restored. To restore alert events in ClickHouse, you need to install a storage with the same storage cluster ID, where in the `kuma.alert_events_local` table, event records can be matched to alerts by IDs. If the storage changes, alert events can be viewed provided that a backup copy is created and then the ClickHouse database is restored.

- Backing up collectors is not necessary, except collectors with an SQL connection. When restoring such collectors, the ID value should be returned to its initial value.

Creating a backup of the KUMA Core

To create a backup copy of KUMA Core in the web interface:

1. In the web interface, in the **Resources** → **Active services** section, select the check box next to the KUMA Core service that has the green status.
2. In the toolbar or menu (⋮), select **Backup** and click **Create a backup copy**.

   This setting is available if one KUMA Core service is selected in green status.

   The option is not available in the following cases:

   - If you have selected a check box next to multiple services.
   - If the KUMA Core service has the red status.
   - If no check boxes are selected.
   - If you have selected a check box next to a service of another type.

   The backup starts automatically. The backup file is saved to the **Downloads** folder or the folder that you configured in your browser for downloaded files. If download completion notification is enabled in your browser settings, a notification will tell you that the backup file was downloaded successfully or that an error occurred.

The backup file name includes the name of the service. If you create a backup copy of the same service multiple times, a copy number in parentheses is appended to the service name. For example, a file saved for the first time is named `core-1`. The file of the next backup copy you create is named `core-1 (1)`.

Metrics are not included in the backup copy.

A backup of KUMA Core is created.

Backing up the KUMA Core using the API

For KUMA 4.0 and later, use API v3.

To create a backup copy and restore the KUMA Core, the user must have access rights to the API methods: `GET /system/backup` and `POST /system/restore`. You also need to create a token for making API requests.

To create a backup of KUMA Core using the API

1. Connect to the CLI of the KUMA server on which the KUMA Core is installed.

2. Send an API request:

```
curl -k --header 'Authorization: Bearer <token>' 'https://<ip_kuma>:7223/api/v3/system/backup' -o backup.tar.gz
```

You will get a `tar.gz` archive containing a backup copy of the KUMA Core. The backup copy is not saved on the host where the Core is installed. Certificates are included in the backup copy. If the operation is successful, an audit event is generated.

Restoring the KUMA Core for a single-server installation

You can restore the KUMA Core from a backup copy only within the same version of KUMA. A version conflict error is returned if attempt to restore KUMA from a backup copy created in a different version of KUMA.

Restoring the KUMA Core without changing the host for core-1

This article describes the procedure for restoring the KUMA Core on the same host on which the KUMA Core was installed.

To restore the KUMA Core from a backup copy, use one of the following methods:

- Using the REST API:

```
curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'
--data-binary '@/backup/backup.tar.gz'
```

- In the web interface:

  1. In the web interface, in the **Resources** → **Active services** section, select the check box next to the KUMA Core service that has the green status.

  2. In the menu (⋮) select **Backup** → **Restore**.

  3. This opens a window; in that window, select the backup file that you want to restore.

  If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

The KUMA Core is restored from the backup, and the web interface login page is displayed.

Restoring the KUMA Core with a change of host for core-1

This article describes how to restore the KUMA Core from a backup copy on a new host.

To restore the KUMA Core from a backup copy:

1. Install KUMA on a single server on a new host using the `install.sh` installer and the `single.inventory.yml` inventory file; set

   ```
   deploy_example_services: false
   ```

   Example single.inventory.yml inventory file

   ```
   all:
     vars:
       deploy_to_k8s: false
       need_transfer: false
       generate_etc_hosts: false
       deploy_example_services: true
       no_firewall_actions: false
   kuma:
     vars:
       ansible_connection: ssh
       ansible_ssh_private_key_file: <full path to the file with the SSH key>
       ansible_user: <user from the sudo group>
       ansible_become: true
       ansible_port: 2222
     children:
       kuma_core:
         hosts:
           kuma1.example.com:
       kuma_collector:
         hosts:
           kuma1.example.com
       kuma_correlator:
         hosts:
           kuma1.example.com
       kuma_storage:
         hosts:
           kuma1.example.com:
             shard: 1
             replica: 1
             keeper: 1
       kuma_metrics:
         hosts:
           kuma1.example.com
   ```

   Only the KUMA Core is installed.

2. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

     ```
     curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-binary '@/backup/backup.tar.gz'
     ```

   - In the web interface:

     a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

     b. This opens a window; in that window, select the backup file that you want to restore.

     If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

3. Reissue the certificates of services. To do this, reset the certificates of all services except the KUMA Core:

   a. In the **Resources** → **Active services** section, select the **Select all** check box, then clear the check box for the KUMA Core service.

   b. In the toolbar or menu (⋮), select **Reset certificate**.

   The certificates are reset and automatically reissued for all services except the KUMA Core. Reissuing certificates for the KUMA Core is not required, since after restoring from a backup, the KUMA Core already contains the necessary data, including information about certificates and trusted services that were restored along with the backup.

4. On the host on which the Metrics service is installed, delete the /opt/kaspersky/kuma/metrics/00000000-0000-0000-0000-000000000000/certificates directory. This is necessary so that the next time the Metrics service starts, it does not use the local data of the previous certificate. You do not need to restart the Metrics service separately. At the next step, the change_url.sh script will reconnect the Metrics service with the new KUMA Core and restart the Metrics service.

5. Reconnect all services to the new KUMA Core and restart all services in one of the following ways:

   - Automatically, using the `change_url.sh` script included in the distribution kit.

     The script reconnects the services installed on the hosts specified in the `distributed.inventory.yml` file en masse and restarts these services. The script processes services that are operational (have a green status) at the time when the script is run.

     a. Update the `distributed.inventory.yml` inventory file by specifying the FQDN of the host to which you moved the KUMA Core in the `kuma_core` section and run the `change_url.sh` script using the following command:

     ```
     ./change_url.sh distributed.inventory.yml
     ```

     The script reconnects all services installed on hosts specified in the `distributed.inventory.yml` inventory file to the new KUMA Core, and also restarts all services.

     Services that were non-operational (had a red status) at the moment when the script was run are not reconnected automatically, even if their status changes to green after that. Reconnect such services manually.

- Manually using a command. Use this method if you need to reconnect an individual service, for example, a service that was not reconnected by the script.

  ```
  sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter/metrics --core https://<FQDN>:<port>
  --pair.fingerprint <CA_cert_ID> --id <service_ID> --api.port <API_port> --install
  ```

  where:

  - <FQDN> is the fully qualified domain name of the KUMA Core server.
  - <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
  - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

    The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
    You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

    To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
  - <service_ID> is the service ID copied from the KUMA web interface.
  - <API_port> is the port used for communication with the component being installed.

The KUMA Core is restored from the backup, and the web interface login page is displayed.

Restoring the KUMA Core for a distributed installation

You can restore the KUMA Core from a backup copy only within the same version of KUMA. A version conflict error is returned if attempt to restore KUMA from a backup copy created in a different version of KUMA.

Restoring the KUMA Core without changing the host for core-1

To restore the KUMA Core from a backup copy, use one of the following methods:

- Using the REST API:

  ```
  curl -k --request POST '<FQDN>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-
  binary '@/backup/backup.tar.gz'
  ```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <token> is the token for API requests.

- In the web interface:

  a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

  b. This opens a window; in that window, select the backup file that you want to restore.

  If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

The KUMA Core is restored from the backup, and the web interface login page is displayed.

After the restoration is complete, KUMA Core continues to work with existing services. You do not need to additionally configure services.

Restoring the KUMA Core with a change of host for core-1

These instructions describe how to restore the KUMA Core from a backup copy on a new host. The rest of KUMA services remain on their old hosts.

After restoration, you need to reissue the service certificates and reconnect the services to the KUMA Core on the new host.

To restore the KUMA Core from a backup copy:

1. Prepare the new KUMA instance by installing KUMA on a single server on a new host using the `install.sh` installer and the `single.inventory.yml` inventory file; set

   ```
   deploy_example_services: false
   ```

   Only the KUMA Core will be installed on the host specified in the inventory file.

   The new KUMA Core instance does not contain data from the old infrastructure. The backup is restored in this instance.

2. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

     ```
     curl -k --request POST '<FQDN>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --
     data-binary '@/backup/backup.tar.gz'
     ```

     where:

     - <FQDN> is the fully qualified domain name of the KUMA Core server.
     - <token> is the token for API requests.

- In the web interface:

  a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

  b. This opens a window; in that window, select the backup file that you want to restore.

  After the restoration is complete, the login page for the KUMA web interface is displayed.

  If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

After restoring the KUMA Core from backup, follow these steps so that services can connect to the KUMA Core on the new host.

3. Reissue the certificates of services. To do this, reset the certificates of all services except the KUMA Core:

   a. In the **Resources** → **Active services** section, select the **Select all** check box, then clear the check box for the KUMA Core service.

   b. In the toolbar or menu (⋮), select **Reset certificate**.

   The certificates are reset and automatically reissued for all services except the KUMA Core. Reissuing certificates for the KUMA Core is not required, since after restoring from a backup, the KUMA Core already contains the necessary data, including information about certificates and trusted services that were restored along with the backup.

4. On the host on which the Metrics service is installed, delete the /opt/kaspersky/kuma/metrics/00000000-0000-0000-0000-000000000000/certificates directory. This is necessary so that the next time the Metrics service starts, it does not use the local data of the previous certificate. You do not need to restart the Metrics service separately. At the next step, the change_url.sh script will reconnect the Metrics service with the new KUMA Core and restart the Metrics service.

5. Reconnect all services to the new KUMA Core and restart all services in one of the following ways:

   - Automatically, using the `change_url.sh` script included in the distribution kit.

     The script reconnects the services installed on the hosts specified in the `distributed.inventory.yml` file en masse and restarts these services. The script processes services that are operational (have a green status) at the time when the script is run.

     a. Update the `distributed.inventory.yml` inventory file by specifying the FQDN of the host to which you moved the KUMA Core in the `kuma_core` section and run the `change_url.sh` script using the following command:

     ```
     ./change_url.sh distributed.inventory.yml
     ```

     The script reconnects all services installed on hosts specified in the `distributed.inventory.yml` inventory file to the new KUMA Core, and also restarts all services.

     Services that were non-operational (had a red status) at the moment when the script was run are not reconnected automatically, even if their status changes to green after that. Reconnect such services manually.

   - Manually using a command. Use this method if you need to reconnect an individual service, for example, a service that was not reconnected by the script.

     ```
     sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter/metrics --core https://<FQDN>:<port>
     ```

```
--pair.fingerprint <CA_cert_ID> --id <service_ID> --api.port <API_port> --install
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the service ID copied from the KUMA web interface.
- <API_port> is the port used for communication with the component being installed.

After the procedure is completed, all KUMA services are connected to the restored KUMA Core on the new host.

Restoring in a Kubernetes cluster

This section describes various fault scenarios and recovery methods, as well as alternative methods using virtual machine snapshots of cluster nodes.

A prerequisite for recovery is the availability of an up-to-date backup copy of the KUMA Core. We also recommend saving your traffic balancer configuration.

Temporary unavailability of individual cluster components

If individual cluster components are temporarily unavailable, for example, due to a temporary server power outage, lack of network connectivity, or a failure that required restarting the server or virtual machine, recovery does not require creating virtual machines from scratch or replacing servers. The availability of the KUMA Core in this case is determined by which components remain in operation (more information about monitoring the health of KUMA Core in a Kubernetes cluster). This scenario also covers failures on a server or virtual machine that do not require reinstalling the operating system and that can be quickly remedied by replacing individual hardware components or changing the software configuration.

After all components are restored and available, the cluster is restored automatically. It takes some time to complete transient operations such as synchronizing volume replicas, during which time the cluster remains vulnerable to new failures of other components. Thus, synchronization of replicas of large volumes can take several hours. This recovery time must be taken into account when planning an exercise with the deliberate shutdown of worker nodes.

Complete failure of cluster components while the availability of the KUMA Core is maintained

Until the next component fails, the cluster lets you continue using the KUMA Core, select a suitable recovery window and create an up-to-date backup of the KUMA Core.

To restore a cluster:

1. Prepare new virtual machines or servers to replace failed cluster components in accordance with the KUMA hardware and software requirements.

   You can also use snapshots of virtual machines taken before installing KUMA.

2. Review the `k0s.inventory.yml` inventory file and update it if necessary. If you have many services and you need to minimize installation time, you can leave one host in the `kuma_collector` and `kuma_correlator` sections, and leave one storage cluster in the `kuma_storage` section. If a host from the `kuma_control_plane_master` section has failed, then in inventory file `k0s.inventory.yml`, you need to swap this host with the cluster controller from the `kuma_control_plane` section.

3. Install the current KUMA version using the `install.sh` script and the prepared `k0s.inventory.yml` inventory file:

   ```
   ./install.sh k0s.inventory.yml
   ```

   The user that will be used to install the solution must have permissions to the installer archive as well as write permissions for the directory in which the archive is to be unpacked.

4. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

     ```
     curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer
     <token>'  --data-binary '@/backup/backup.tar.gz'
     ```

   - In the web interface:

     a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

     b. This opens a window; in that window, select the backup file that you want to restore.

     If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

   KUMA Core is restored and the KUMA web interface login page is displayed.

5. Make sure that all cluster components are working properly and that high availability is restored:

   a. All `k0s` services are running:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

b. Information about pods and all working nodes is available:

```
View volume status
sudo k0s kubectl get volume -n longhorn-system -o json | jq '.items[0].status.robustness'
```

The status must be `healthy`. If the status is `degraded`, then one of the replicas is unavailable or is being restored.

```
Monitor the volume recovery process
sudo k0s kubectl get engine -n longhorn-system -o json | jq '.items[0].status.rebuildStatus'
```

If it is working correctly, recovery is not being performed, and the command does not return anything. If the command returns the `rebuilding` status, it means that some replicas are in the process of being rebuilt. We recommend not making any changes to the cluster until the rebuilding is complete.

6. Install the Metrics service using the `expand.sh` installer and the `expand.inventory.yml` inventory file. Transfer the data from the `metrics` directory to the host with the restored KUMA Core.

The cluster is restored.

Complete failure of cluster components with the KUMA Core unavailable

> You must have a backup of the KUMA Core on hand.

To restore a cluster, you must first delete the cluster that is in use.

To restore a cluster:

1. Prepare new virtual machines or servers to replace failed cluster components in accordance with the KUMA hardware and software requirements.

   You can also use snapshots of virtual machines taken before installing KUMA.

2. Prepare a separate `k0s.inventory.yml` inventory file for cluster deletion. In this inventory file, remove all hosts from the `kuma_collector`, `kuma_correlator`, and `kuma_storage` sections to avoid having to uninstall and then reinstall services.

3. Remove the failed cluster:

   a. Run the `uninstall.sh` installer with the prepared `k0s.inventory.yml` inventory file:

   ```
   ./uninstall.sh k0s.inventory.yml
   ```

   b. Restart all hosts specified in the `kuma_worker*` and `kuma_control_plane*` sections.

   c. After the hosts have booted, run `uninstall.sh` again with the `k0s.inventory.yml` inventory file:

   ```
   ./uninstall.sh k0s.inventory.yml
   ```

4. Prepare the KUMA inventory file for cluster recovery. Take the current inventory file for installation as a basis.

   If you have many external services and you need to minimize installation time, you can leave one host in the `kuma_collector` and `kuma_correlator` sections, and leave one storage cluster in the `kuma_storage` section.

   If you do not need to minimize the installation time and restarting of external KUMA services is permissible, then you can use the inventory file without modifications.

5. Install the current KUMA version using the `install.sh` script and the prepared `k0s.inventory.yml` inventory file to restore the cluster:

6. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

     ```
     curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-binary '@/backup/backup.tar.gz'
     ```

   - In the web interface:

     a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

     b. This opens a window; in that window, select the backup file that you want to restore.

     If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

   KUMA Core is restored and the web interface login page is displayed.

7. Make sure that the KUMA Core and other KUMA services are working properly. To do this, go to the **Resources** → **Active services** section. All services must have the green status.

8. Make sure that all cluster components are working properly and that high availability is restored:

   a. All `k0s` services are running:

   ```
   sudo systemctl status <k0sworker/k0scontroller>
   sudo k0s status
   ```

b. Information about pods and all working nodes is available:

```
View volume status
sudo k0s kubectl get volume -n longhorn-system -o json | jq '.items[0].status.robustness'
```

The status must be `healthy`. If the status is `degraded`, then one of the replicas is unavailable or is being restored.

```
Monitor the volume recovery process
sudo k0s kubectl get engine -n longhorn-system -o json | jq '.items[0].status.rebuildStatus'
```

If it is working correctly, recovery is not being performed, and the command does not return anything. If the command returns the `rebuilding` status, it means that some replicas are in the process of being rebuilt. We recommend not making any changes to the cluster until the rebuilding is complete.

9. Install the Metrics service using the `expand.sh` installer and the `expand.inventory.yml` inventory file. Transfer the data from the `metrics` directory to the host with the restored KUMA Core.

The cluster is restored.

Failure of the traffic balancer

If the traffic balancer fails, the KUMA Core becomes unavailable. However, to restore the balancer, you do not need to delete or change the existing cluster or KUMA services. If you have a snapshot of the balancer virtual machine taken after installing KUMA, you can use this snapshot. If you do not have a virtual machine snapshot or if you want to use a new server to replace the failed one, to restore the cluster, you need to install the balancer and configure it using the previously saved configuration.

After the traffic balancer is recovered, access to the cluster and the KUMA Core is restored.

Using snapshots of virtual machines for the members of the Kubernetes cluster

Traffic balancer

After initial configuration, the load balancer is a stateless host. To save state, you can take a snapshot of its virtual machine at any time after installing the current version of KUMA. Likewise, the virtual machine can be restored from a snapshot at any time, as long as that the KUMA version of the virtual machine snapshot is the same as the current KUMA version. If the versions are different, the traffic balancer configuration file may need to be edited to reflect any changes in the list of served ports.

Limitations:

- Depending on the type of your hypervisor, at the time of creating a snapshot of the virtual machine, current connections may be interrupted.
- Restoring from a snapshot breaks current connections.
- From the moment when the virtual machine is restored from a snapshot and until new connections are established, the KUMA Core is unavailable.

Cluster controller

Controllers manage the cluster. During the operation of the cluster, the quorum of the controllers must be maintained at all times.

A controller may be shut down for a short time as long as overall quorum is maintained. Controller virtual machine snapshots can be created one by one. However, if the creation of the snapshot causes temporary unavailability of `k0s` services (depending on the hypervisor), enough time must be allowed between snapshots for the consensus to be restored and for the etcd database of the cluster to be re-synchronized.

Limitations:

- Restoring one or more controllers from a virtual machine snapshot while the cluster is running will lead to undefined behavior.
- A controller virtual machine snapshot may only be used to restore the virtual machine before completely removing the KUMA Core cluster and then reinstalling the KUMA Core from scratch and recovering from a backup copy.

Worker node of the cluster

Worker nodes of the cluster run the KUMA Core and store replicas of the persistent storage volume used by the KUMA Core services. Creating virtual machine snapshots negatively affects the state of the storage volume; from the errors in the replica with automatic re-creation of the replica to errors in the file system that necessitate completely shutting down the volume and stopping KUMA Core pods. The consequences depend on the type of hypervisor, the operating system of the virtual machine, the state of all replicas and the intensity of disk operations at the time when the snapshot is created.

Limitations:

Restoring a worker node from a virtual machine snapshot while the cluster is running can lead to the cluster becoming inoperable. Even using a snapshot of a temporarily decommissioned working node does not allow the re-introduction of such a node into the cluster after restoring its virtual machine. Snapshots of worker nodes taken just before the installation of the KUMA Core can be useful. Such snapshots may facilitate the preparation of the KUMA Core reinstallation during recovery.

Restoring in a Raft cluster

This section describes how to restore KUMA Core on a Raft cluster, a Raft cluster node, or a Raft cluster.

You can restore the KUMA Core from a backup copy only within the same version of KUMA. A version conflict error is returned if attempt to restore KUMA from a backup copy created in a different version of KUMA.

Restoring the KUMA Core without changing the host for core-1

This manual describes how to restore KUMA Core from a backup on the host specified in the `kuma_core` section, that is, the host on which KUMA Core has been installed.

To restore the KUMA Core from a backup copy:

1. Prepare the cluster for recovery. To do this, on each host specified in the inventory file in the `kuma_core_peers` section:

   a. In the web interface, go to the **Resources and services** → **Active services** section.

   b. Select the check box next to the KUMA Core service and in the toolbar or in the menu (⋮), select **Copy ID**.

   You will need the ID of the KUMA Core service to stop the service on the host.

   c. Select the check box next to the KUMA Core service and in the toolbar or in the menu (⋮), click **Delete**.

   d. On the Raft cluster host where the KUMA Core service is installed, stop the KUMA Core service by running the following command on the command line:

   ```
   sudo systemctl stop kuma-core-<KUMA Core service ID>.service
   ```

   e. On each Raft cluster host where the KUMA Core service is installed, delete the working directory:

   ```
   sudo rmdir <directory_name>
   ```

   f. On the Raft cluster host where the KUMA Core service is installed, remove the `systemd` service.

   All KUMA Core services are stopped and the servers are ready for cluster recovery.

2. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

   ```
   curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer
   <token>'  --data-binary '@/backup/backup.tar.gz'
   ```

   - In the web interface:

     a. In the web interface, open the **Resources and services** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

     b. This opens a window; in that window, select the backup file that you want to restore.

     If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

   KUMA Core is restored and the web interface login page is displayed.

3. If you need a high-availability Raft cluster, restore the rest of the cluster nodes:

   - If you want to add servers for KUMA Core services, use the `expand.sh` installer and the `expand.inventory.yml` inventory file to expand the Raft cluster.

   - If you are using your old nodes:

     a. Get the service ID. To do this, in the web interface, go to **Resources** → **Active services**, and in the context menu of the KUMA Core, click **Copy ID**.

     b. Reinstall the KUMA Core services by specifying the `--raft.join` parameter to add the nodes to the Raft cluster, using the following command:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN of the initial cluster node>:7210 --
     pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <ID of the KUMA Core service> --
     install
     ```

     where:

     `<fingerprint ID of the KUMA Core CA certificate>` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

     The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
     You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

     To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

4. Install the Metrics service using the `expand.sh` installer and the `expand.inventory.yml` inventory file. Transfer the data from the `metrics` directory to the host of the restored KUMA Core.

KUMA Core is restored from the backup.

Restoring the KUMA Core with a change of host for core-1

These instructions describe how to restore the KUMA Core from a backup copy on a new host.

To restore the KUMA Core from a backup copy:

1. Prepare the cluster for recovery. To do this, on all Raft cluster hosts, do the following:

   a. In the web interface, go to the **Resources and services** → **Active services** section.

   b. Select the check box next to the KUMA Core service and in the toolbar or in the menu (⋮), click **Copy ID**.

   You will need the ID of the KUMA Core service to stop the service on the host.

   c. Select the check box next to the KUMA Core service and in the toolbar or in the menu (⋮), click **Delete**.

d. On the Raft cluster host where the KUMA Core service is installed, stop the KUMA Core service by running the following command:

```
sudo systemctl stop kuma-core-<ID of the KUMA Core service copied from the web interface>.service
```

e. On each Raft cluster host where the KUMA Core service is installed, delete the working directory:

```
sudo rmdir <directory_name>
```

f. On the Raft cluster host where the KUMA Core service is installed, remove the `systemd` service.

All KUMA Core services are stopped and the servers are ready for cluster recovery.

2. Perform a single-server installation of KUMA on a new host using the `install.sh` installer and the `single.inventory.yml` inventory file; set `deploy_example_services: false`.

   Only the KUMA Core will be installed on the host specified in the inventory file.

3. Restore the KUMA Core from a backup copy in one of the following ways:

   - Using the REST API:

     ```
     curl -k --request POST 'https://<ip_kuma>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>'  --data-binary '@/backup/backup.tar.gz'
     ```

   - In the web interface:

     a. In the web interface, open the **Resources** → **Active services** section and in the menu (⋮), select **Backup** → **Restore**.

     b. This opens a window; in that window, select the backup file that you want to restore.

     If notifications are configured in your browser, a message is displayed in the upper-right corner, telling you that the **KUMA Core is successfully restored**.

   The initial cluster node with KUMA Core is restored and the web interface login page is displayed.

4. If you need a high-availability Raft cluster, perform the restoration procedure on the rest of the cluster nodes:

   - If you want to add servers for KUMA Core services, use the `expand.sh` installer and the `expand.inventory.yml` inventory file to expand the Raft cluster.

   - If you are using your old nodes:

     a. Get the service ID. To do this, in the web interface, go to **Resources** → **Active services**, and in the context menu of the KUMA Core, click **Copy ID**.

     b. Reinstall the KUMA Core services by specifying the `--raft.join` parameter to add the nodes to the Raft cluster, using the following command:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN of the initial cluster node>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
     ```

     where:

`< fingerprint ID of the KUMA Core CA certificate >` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

5. Reconnect the services to the new KUMA Core using the following command:

```
sudo /opt/kaspersky/kuma/kuma collector/correlator/storage/eventRouter --core https://<KUMA Core server FQDN>:
<port used by KUMA Core server for internal communication (port 7210 by default)> --pair.fingerprint
<fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <port for communication with the
installed component> --install
```

6. Install the Metrics service using the `expand.sh` installer and the `expand.inventory.yml` inventory file. Transfer the data from the `metrics` directory to the host with the restored KUMA Core.

7. Reconfigure the load balancer by specifying the hosts on which the KUMA Core service is installed.

The restoration from a backup copy is completed.

Restoring a Raft cluster node

If one or more nodes are damaged but the cluster remains healthy, you can restore the Raft cluster nodes.

Restoring the nodes of the Raft cluster consists of the following steps:

1. **Removing a node from the Raft cluster**

   Remove the corrupted node from the Raft cluster.

2. **Create a node with the KUMA Core service and add it to the cluster using the --raft.join option**

   Add a new node with the KUMA Core service. To do this, create a node using the `expand.sh` installer and the `expand.inventory.yml` inventory file. Then create in the web interface and install a new KUMA Core service on the server specified in the `expand.inventory.yml` inventory file under the `kuma_core_peers` section using the installation command with the `--raft.join` parameter. After this, a new node will be added to the Raft cluster.

The new node gets a complete copy of the state of the leader node. However, temporary files, including artifacts of background tasks that may have been present on the damaged node, are not restored.

Restoring the Raft cluster

If most of the nodes in the Raft cluster are corrupted and the cluster is inoperable, the following recovery methods are available:

From the current state of the selected node

To restore the Raft cluster from the current state of a selected node:

1. Prepare the cluster for recovery:

   a. Choose the node to become the initial node of the new cluster. On this node, you need to stop the KUMA Core service, but without deleting the working directory and the `systemd` file.

   b. Stop the KUMA Core service on all nodes in the cluster:

   ```
   sudo systemctl stop kuma-core-<KUMA_Core_service_ID>.service
   ```

   c. Delete the working directories on all nodes in the cluster except the chosen initial node:

   ```
   sudo rmdir <directory_name>
   ```

   d. On all nodes in the cluster except the initial node, remove the `systemd` services.

   All KUMA Core services are stopped. The servers are ready for cluster recovery.

2. Restore the Raft cluster with a single KUMA Core:

   a. On the initial node of the new Raft cluster, create the following file:

   ```
   sudo touch /opt/kaspersky/kuma/core/<service_id>/raft/.reset
   ```

   b. On the initial node of the Raft cluster, remove the `--raft.join` parameter in the `systemd` file and apply the changes by running the following command:

   ```
   sudo systemctl daemon-reload
   ```

   c. On the initial node of the Raft cluster, start the KUMA Core:

   ```
   sudo systemctl start kuma-core-<KUMA Core service ID>.service
   ```

   The Raft cluster is restored with a single KUMA Core. On the rest of the nodes, the KUMA core services are stopped and the nodes are removed from the cluster.

3. If you need a high-availability Raft cluster, restore the rest of the cluster nodes:

   - If you want to add servers for KUMA Core services, use the `expand.sh` installer and the `expand.inventory.yml` inventory file to expand the Raft cluster.

   - If you are using your old nodes:

     a. Get the service ID. To do this, in the web interface, go to **Resources** → **Active services**, and in the context menu of the KUMA Core, click **Copy ID**.

     b. Reinstall the KUMA Core services by specifying the `--raft.join` parameter to add the nodes to the Raft cluster, using the following command:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN of the initial cluster node>:7210 --id <ID of the
     KUMA Core service> --install
     ```

   The cluster is restored. Certificates of services, such as collectors, correlators, and storages, do not need to be reset.

Using a backup

> A backup does not contain temporary files, including artifacts of background tasks.

To restore the Raft cluster from backup:

1. Prepare the cluster for recovery:

   a. Stop the KUMA Core service on each node in the cluster:

   ```
   sudo systemctl stop kuma-core-<KUMA_Core_service_ID>.service
   ```

   b. On each node where the KUMA Core service is installed, delete the working directory:

   ```
   sudo rmdir <directory_name>
   ```

   c. On each node where the KUMA Core service is installed, remove the `systemd` service.

   All KUMA Core services are stopped. The servers are ready for cluster recovery.

2. Restore the Raft cluster with a single KUMA Core:

   a. Select the server that will become the new initial node of the Raft cluster and deploy the new initial node of the cluster without the `--raft.join` option:

   ```
   sudo /opt/kaspersky/kuma/kuma core --raft.node.listen 0.0.0.0:7209 --raft.node.addr "$(hostname -f):7209" -
   -health 0.0.0.0:7208 --internal 0.0.0.0:7210 --private 0.0.0.0:7220 --cybertrace 0.0.0.0:7222 --rest
   0.0.0.0:7223 --install
   ```

   b. Restore from backup using the REST API.

   The Raft cluster is restored from backup. The initial node of the KUMA Core cluster is restored.

3. If you need a high-availability Raft cluster, perform the restoration procedure on the rest of the cluster nodes:

   - If you want to add servers for KUMA Core services, use the `expand.sh` installer and the `expand.inventory.yml` inventory file to expand the Raft cluster.

   - If you are using your old nodes:

     a. Get the service ID. To do this, in the web interface, go to **Resources** → **Active services**, and in the context menu of the KUMA Core, click **Copy ID**.

     b. Reinstall the KUMA Core services by specifying the `--raft.join` parameter to add the nodes to the Raft cluster, using the following command:

     ```
     sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN of the initial cluster node>:7210 --id <ID of the
     KUMA Core service> --install
     ```

The cluster is restored. Certificates of services, such as collectors, correlators, and storages, do not need to be reset. If the list of cluster nodes has changed after recovery, change the value of the `--core` parameter in the `systemd` file to make the services access the KUMA Core that you need.

Maintenance of hosts in a Kubernetes cluster

Sometimes you need to restart, install updates, or update the operating system on worker nodes and controllers of the Kubernetes cluster. This article describes a host maintenance procedure that minimizes the downtime of the KUMA Core in a high-availability configuration.

Before taking hosts out for maintenance, you need to create a backup copy of the KUMA core.

Controller maintenance

Cluster controllers must undergo maintenance one at a time. No action is required before performing maintenance of a controller. After maintenance or an upgrade, you must make sure that the controller has started successfully by checking the status of the service using the following commands:

```
sudo systemctl status k0scontroller
sudo k0s status
```

After the controller comes back up after maintenance, you can perform maintenance of the next controller. As long as you perform maintenance of controllers one by one, KUMA Core remains available.

Maintenance of working nodes

Worker nodes of the cluster must be taken out for maintenance strictly one at a time.

To perform maintenance on worker nodes:

1. Get the names and current status of worker nodes by running the following command on any controller:

   ```
   sudo k0s kubectl get nodes
   ```

   All worker nodes must have the `ready` status, otherwise the decommissioning of more nodes may lead to unavailability of the KUMA Core.

2. Before upgrading a worker node, prevent pods from being placed on this node by running the following command:

   ```
   sudo k0s kubectl cordon <worker_node_name>
   ```

   After that, the output of the `sudo k0s kubectl get nodes` command shows the node with the `Ready,SchedulingDisabled` status.

3. Get the name of the worker node on which the KUMA Core is running by running the following command on any controller:

   ```
   sudo k0s kubectl get pods -n kuma -o wide
   ```

4. If the KUMA Core is running on the worker node which is undergoing maintenance, restart the KUMA Core deployment to move the KUMA Core to another worker node, and wait until the KUMA Core is successfully started on the other worker node. To restart the deployment of the KUMA Core, run the following command:

   ```
   sudo k0s kubectl rollout restart deployment core-deployment -n kuma
   ```

   While the KUMA Core is being moved to another worker node, the KUMA Core is unavailable for approximately 10 minutes.

5. Check the status of the KUMA Core by running the following command again:

   ```
   sudo k0s kubectl get pods -n kuma -o wide
   ```

   The pod should have the `Running` status. The name of the worker node in the `NODE` column should change.

6. Stop the `k0sworker` service on the node that you are taking out with the following command:

   ```
   sudo k0s stop
   ```

7. Update the operating system.

8. Start the `k0s` service on the worker node with the following command:

   ```
   sudo k0s start
   ```

9. Make sure that the `k0s` service has started successfully by running the following commands on the worker node:

   ```
   sudo systemctl status k0sworker
   sudo k0s status
   ```

   The `k0sworker.service` must be in the `active (running)` state.

   The `k0s status` command should return `Status: Running`.

10. Allow pods to be run on the updated worker node by running the following command on any controller:

    ```
    sudo k0s kubectl uncordon <worker_node_name>
    ```

11. Make sure that the worker node in the cluster is available by running the following command on any controller:

    ```
    sudo k0s kubectl get nodes
    ```

    The upgraded worker node should have the `ready` status.

12. After returning the working node to the cluster, make sure that all volume replicas are restored and available by running the following command:

    ```
    sudo k0s kubectl get volume -n longhorn-system -o json | jq '.items[0].status.robustness'
    ```

    The status must be `healthy`. If the status is `degraded`, then one of the replicas is unavailable or is being rebuilt.

13. If you want to monitor the volume rebuilding process, run the following command:

    ```
    sudo k0s kubectl get engine -n longhorn-system -o json | jq '.items[0].status.rebuildStatus'
    ```

14. If you want to view the current status of replicas, run the following command:

    ```
    sudo k0s kubectl get replicas -n longhorn-system
    ```

    All replicas must have the `running` status.

Worker node maintenance is complete. If the serviced worker node is ready and the KUMA Core volume has the `healthy` status, you can proceed to perform maintenance on the next worker node.

Maintenance of the traffic balancer

Maintenance of the traffic balancer always results in the KUMA Core becoming temporarily unavailable, both for users and for KUMA services. While the balancer is unavailable, a KUMA Core pot cannot be moved from one worker node to another.

If you are planning a long downtime of the main balancer or substantial upgrades, we recommend the following:

1. Prepare a backup balancer with all necessary updates, duplicate the configuration of NGINX or other traffic balancer that you are using from your main balancer to the backup balancer. For NGINX configured by the KUMA installer, the relevant files are `/etc/nginx/nginx.conf` and `/etc/nginx/kuma_nginx_lb.conf`.

   The FQDN of the backup balancer must be the same as the FQDN of the main balancer. Make sure that the balancer service has started successfully and that the firewall rules applied to the main balancer are also applicable to the backup load balancer.

2. Switch traffic over to the backup balancer by changing the IP address of the backup balancer to the IP address of the main balancer. On the main balancer, change the IP address to some other IP address to prevent IP address conflict. Make sure that the KUMA Core on the backup balancer is working properly.

   > When you switch over the traffic, current sessions may be terminated. In case of any problems, you can specify the old IP addresses and continue using the main balancer in the previous configuration.

3. Perform maintenance on the main balancer as necessary.

4. Change the IP addresses on the main and backup balancers to their old values.

5. Make sure that the KUMA Core on the updated main balancer is working properly.

   The last step may not be necessary if you want to discard the old main balancer, that is, if you are permanently replacing the balancer with an updated host.

The resource requirements of the traffic balancer are minimal, therefore we recommend having a backup clone of the balancer virtual machine on hand to quickly restore the availability of the KUMA Core in case of any problems with the main virtual machine.

Modifying a previously deployed configuration

This section describes the steps for modifying a previously deployed KUMA configuration.

Expanding a single-server deployment configuration to a distributed configuration

This article describes how to expand a single-server deployment configuration to a distributed configuration, and provides an example of expanding the configuration.

The transition to a distributed deployment scheme may be required in the following cases:

- For load balancing when load exceeds the recommended level and performance decreases.
- Ensuring high fault tolerance of all components.
- Requirements for high availability of storage services (a large number of complex search requests).

- IT infrastructure features, such as isolated network segments with low-bandwidth communication channels.
- Administrative features. For example, there are requirements to share access between the teams–server administrator, requirements of regulators–local data storage.

To expand a single-server deployment configuration to a distributed configuration:

1. Create a backup copy of KUMA.
2. Prepare the target computers to expand a single-server deployment configuration to a distributed configuration.
3. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

   ```
   cd kuma-ansible-installer
   ```

4. Prepare the `expand.inventory.yml` inventory file:

   a. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

   b. In the `expand.inventory.yml` inventory file, in the `kuma_<component name>` sections, enter the FQDNs of the target computers for installing KUMA services.

5. On the control computer, run the following command as root from the directory with the extracted installer:

   ```
   ./expand.sh expand.inventory.yml
   ```

   This command creates installation files of KUMA services on each target computer specified in `expand.inventory.yml`.

6. Reset the certificates for the services that you want to migrate to the target computers specified in the `expand.inventory.yml` inventory file:

   a. In the KUMA web interface, go to the **Resources and services** → **Active services** section.

   b. In the list of services, select the check boxes for the required services and in the context menu, select **Reset certificate**.

   KUMA automatically generates a new certificate for each service for which the certificate has been reset.

7. On the target computers specified in the `expand.inventory.yml` inventory file, install the server parts of KUMA services, server and web parts of which have already been created for the single-server deployment configuration: storages, collectors, correlators, and other necessary services.

8. Restart the KUMA services whose server parts were installed at the previous step:

   a. In the KUMA web interface, go to the **Resources and services** → **Active services** section.

   b. In the list of services, select the check boxes for the required services and in the context menu, select **Restart**.

9. In the `distributed.inventory.yml` inventory file, specify the FQDNs of the target computers added to the configuration so that the file contains up-to-date information in case of a KUMA upgrade.

Example expansion of a single-server deployment configuration to a distributed configuration

A single-server KUMA configuration is deployed in the organization: `kuma.example.com`. The organization's information security officers came to the conclusion that one server is not enough and two additional storage servers and an additional collector server must be added: `storage-1.example.com`, `storage-2.example.com`, and `remote-collector.example.com`.

To make it so, you need to expand the single-server KUMA configuration to a distributed configuration:

1. Create a backup copy of KUMA.

2. Prepare the target computers (`storage-1.example.com`, `storage-2.example.com`, and `remote-collector.example.com`) for adding new storage servers and a collector server to the KUMA configuration.

3. Prepare the `expand.inventory.yml` inventory file:

   a. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

   ```
   cp expand.inventory.yml.template expand.inventory.yml
   ```

   b. In the `expand.inventory.yml` `kuma_<component name>` file, enter the FQDNs of your target computers for installing storage services, collectors, and other required servers.

Example expand.inventory.yml file for adding new storage servers and collector servers

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
      hosts:
        remote-collector.example.com:
          ip: 0.0.0.0
    kuma_correlator:
```

```
      hosts:
        kuma.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 0
          keeper: 1
        storage-1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 0
          keeper: 0
        storage-2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
```

4. On the `kuma.example.com` control computer, run the following command as root from the directory with the extracted installer:

   ```
   ./expand.sh expand.inventory.yml
   ```

   Running this command on each target computer specified in the `expand.inventory.yml` inventory file creates files for creating and installing KUMA services.

5. Reset the certificates for the storage and collector services that you want to migrate to the target computers specified in the `expand.inventory.yml` inventory file:

   a. In the KUMA web interface, go to the **Resources and services** → **Active services** section.

   b. In the list of services, select the check boxes for the storage and collector services and in the context menu, select **Reset certificate**.

   KUMA automatically generates new certificates for the storage and collector services.

6. On the target computers specified in the `expand.inventory.yml` inventory file, install the server parts of the storage and collector, server and web parts of which have already been created for the single-server deployment configuration.

7. Restart the storage and collector services:

   a. In the KUMA web interface, go to the **Resources and services** → **Active services** section.

   b. In the list of services, select the check boxes for the storage and collector services and in the context menu, select **Restart**.

8. If necessary, create destinations with up-to-date information about storages and collectors.

9. In the `distributed.inventory.yml` inventory file, specify the FQDNs of the target computers added to the configuration so that the file contains up-to-date information in case of a KUMA upgrade.

The expansion of a single-server deployment configuration to a distributed configuration is completed.

Adding servers for collectors to a distributed installation

This article describes how to add one or more servers to an existing infrastructure to then install collectors on these servers to balance the load. You can use these instructions as an example and adapt them to your requirements.

To add servers to a distributed installation:

1. Make sure that the target computers meet hardware and software requirements, as well as the requirements for devices with Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS operating systems.

2. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

```
cd kuma-ansible-installer
```

3. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Edit the settings in the `expand.inventory.yml` inventory file and specify the servers that you want to add in the `kuma_collector` section.

   Example expand.inventory.yml inventory file for adding collector servers

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
      hosts:
        kuma-additional-collector1.example.com:
          ip: 0.0.0.0
        kuma-additional-collector2.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
    kuma_storage:
      hosts:
```

5. On the control computer, run the following command as root from the directory with the extracted installer:

```
./expand.sh expand.inventory.yml
```

   This command creates files for creating and installing the collector on each target computer specified in the `expand.inventory.yml` inventory file.

6. Create and install the collectors. KUMA collectors are composed of a client part and a server part, therefore you need to follow these two steps:

   a. Create the client part of the collector, which includes a resource set and the collector service.

To create a resource set for a collector, in the KUMA web interface, under **Resources** → **Collectors**, click **Add collector** and edit the settings. For more details, see Creating a collector.

At the last step of the configuration wizard, after you click **Create and save**, a resource set for the collector is created and the collector service is automatically created. The command for installing the service on the server is also automatically generated. This command is displayed on the screen. Copy the installation command and proceed to the next step.

b. Create the server side of the collector by running the command that you copied at the previous step on the target machine.

The command looks as follows, but all parameters are filled in automatically:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --install
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the service ID copied from the KUMA web interface.

The collector service is installed on the target computer. You can check the status of the service in the web interface under **Resources** → **Active services**.

Run the collector service installation command on each target machine listed in the `kuma_collector` section of the `expand.inventory.yml` inventory file, one machine at a time. On each machine, specify the ID of the relevant collector service in the installation command.

7. Specify the added servers in the `distributed.inventory.yml` inventory file so that it has up-to-date information in case of a KUMA update.

Servers are successfully added.

Adding servers for correlators to a distributed installation

This article describes how to add one or more servers to an existing infrastructure to then install the correlator on these servers to balance the load. You can use these instructions as an example and adapt them to your requirements.

To add servers to a distributed installation:

1. Make sure that the target computers meet hardware and software requirements, as well as the requirements for devices with Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS operating systems.

2. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

```
cd kuma-ansible-installer
```

3. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Edit the settings in the `expand.inventory.yml` inventory file and specify the servers that you want to add in the `kuma_correlator` section.

   Example expand.inventory.yml inventory file for adding correlator servers

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
      hosts:
        kuma-additional-correlator1.example.com:
          ip: 0.0.0.0
        kuma-additional-correlator2.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
```

5. On the control computer, run the following command as root from the directory with the extracted installer:

```
./expand.sh expand.inventory.yml
```

   This command creates files for creating and installing the correlator on each target computer specified in the `expand.inventory.yml` inventory file.

6. Create and install the correlators. KUMA correlators are composed of a client part and a server part, therefore you need to follow these two steps:

   a. Create the client part of the correlator, which includes a resource set and the correlator service.

      To create a resource set for a correlator, in the KUMA web interface, under **Resources** → **Correlators**, click **Add correlator** and edit the settings. For more details, see Creating a correlator.

      At the last step of the configuration wizard, after you click **Create and save**, a resource set for the correlator is created and the correlator service is automatically created. The command for installing the service on the server is also automatically generated. This command is displayed on the screen. Copy the installation command and proceed to the next step.

   b. Create the server side of the correlator by running the command that you copied at the previous step on the target machine.

The command looks as follows, but all parameter values are assigned automatically:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --install
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

- <service_ID> is the service ID copied from the KUMA web interface.

The correlator service is installed on the target computer. You can check the status of the service in the web interface under **Resources** → **Active services**.

Run the correlator service installation command on each target machine listed in the `kuma_correlator` section of the `expand.inventory.yml` inventory file, one machine at a time. On each machine, specify the ID of the relevant correlator service in the installation command.

7. Specify the added servers in the `distributed.inventory.yml` inventory file so that it has up-to-date information in case of a KUMA update.

Servers are successfully added.

Adding servers to an existing storage cluster

This article describes how to add multiple servers to an existing storage cluster. You can use these instructions as an example and adapt them to your requirements.

To add servers to an existing storage cluster:

1. Make sure that the target computers meet hardware and software requirements, as well as the requirements for devices with Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS operating systems.

2. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

```
cd kuma-ansible-installer
```

3. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Edit the settings in the `expand.inventory.yml` inventory file and specify the servers that you want to add in the `storage` section. In the example, the `storage` section specifies servers for installing two shards, each of which contains two replicas. In the `expand.inventory.yml` inventory file, specify only the FQDN. You will assign the roles of shards and replicas in the KUMA web interface at later steps of the instructions. You can adapt this example file to your needs.

   Example expand.inventory.yml inventory file for adding servers to an existing storage cluster

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server8.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server9.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server10.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster1-server11.example.com:
 ip: 0.0.0.0
```

5. On the control computer, run the following command as root from the directory with the extracted installer:

```
./expand.sh expand.inventory.yml
```

   Running this command on each target computer specified in the `expand.inventory.yml` inventory file creates files for creating and installing the storage.

6. You do not need to create a separate storage because you are adding servers to an existing storage cluster. Edit the storage settings of the existing cluster:

   a. In the KUMA web interface, in the **Resources** → **Storages** section, select an existing storage and open it for editing.

   b. In the **ClickHouse cluster nodes** section, click **Add nodes** and specify roles in the fields for the new node. The example describes how to specify IDs to add two shards, containing two replicas each, to an existing cluster. You can adapt this example according to your needs.

   Example of adding nodes

   ```
   ClickHouse cluster nodes
   <existing nodes>
   FQDN: kuma-storage-cluster1server8.example.com
   Shard ID: 1
   Replica ID: 1
   Keeper ID: 0
   FQDN: kuma-storage-cluster1server9.example.com
   Shard ID: 1
   Replica ID: 2
   Keeper ID: 0
   FQDN: kuma-storage-cluster1server9.example.com
   Shard ID: 2
   Replica ID: 1
   Keeper ID: 0
   FQDN: kuma-storage-cluster1server10.example.com
   Shard ID: 2
   Replica ID: 2
   Keeper ID: 0
   ```

   c. Save the storage settings.

   Now you can create storage services for each ClickHouse cluster node.

7. Create a storage service:

   a. In the KUMA web interface, under **Resources** → **Active services**, click **Add service**.

   b. This opens the **Choose a service** window; in that window, select the storage you edited at the previous step and click **Create service**. Do the same for each ClickHouse storage node you are adding.

   The number of created services must be the same as the number of nodes being added to the ClickHouse cluster, for example, 4 services for 4 nodes. The created storage services are displayed in the KUMA web interface in the **Resources** → **Active services** section.

8. Install storage services on each server:

   a. In the KUMA web interface, in the **Resources** → **Active services** section, select the storage service that you need and click **Copy ID**.

   The service ID is copied to the clipboard; you will need it for running the service installation command.

   b. Run the following command on the target computer:

   ```
   sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
   <service_ID> --install
   ```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

- <service_ID> is the service ID copied from the KUMA web interface.

The storage service is installed on the target computer. You can check the status of the service in the web interface under **Resources** → **Active services**.

Run the storage service installation command on each target computer listed in the 'storage' section of the `expand.inventory.yml` inventory file, one computer at a time. On each computer, the unique service ID within the cluster must be specified in the installation command.

9. Apply the changes to the running cluster. To do so, in the KUMA web interface, under **Resources** → **Active services**, select the check boxes next to all storage services in the cluster that you are expanding and click **Update configuration**. Changes are applied without stopping services.

10. Specify the added servers in the `distributed.inventory.yml` inventory file so that it has up-to-date information in case of a KUMA update.

Servers are successfully added to a storage cluster.

Adding another storage cluster

The following instructions describe how to add an extra storage cluster to an existing infrastructure. You can use these instructions as an example and adapt them to suit your needs.

To add a storage cluster:

1. Make sure that the target computers meet hardware and software requirements, as well as the requirements for devices with Oracle Linux, Astra Linux, Ubuntu, RED OS, and Mos OS operating systems.

2. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

```
cd kuma-ansible-installer
```

3. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Edit the settings in the `expand.inventory.yml` inventory file and specify the servers that you want to add in the `storage` section. In the following example, the `storage` section specifies servers for installing 3 dedicated keepers and 2 shards, each of which contains 2 replicas. In the `expand.inventory.yml` inventory file, specify only the FQDN. You will assign the roles of keepers, shards, and replicas in the KUMA web interface at later steps of the instructions. You can adapt this example to suit your needs.

   Example expand.inventory.yml inventory file for adding a storage cluster

```
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_collector:
    kuma_correlator:
    kuma_storage:
      hosts:
        kuma-storage-cluster2-server1.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server2.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server3.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server4.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server5.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server6.example.com:
          ip: 0.0.0.0
        kuma-storage-cluster2-server7.example.com:
          ip: 0.0.0.0
```

5. On the control computer, run the following command as root from the directory with the extracted installer:

```
./expand.sh expand.inventory.yml
```

   Running this command on each target computer specified in the `expand.inventory.yml` inventory file creates files for creating and installing the storage.

6. Create and install the storage. For each storage cluster, you must create a separate storage, that is, 3 storages for 3 storage clusters. A storage is composed of a client part and a server part, therefore you need to follow these two steps:

   a. Create the client part of the storage, which includes a resource set and the storage service:

      1. To create a resource set for a storage, in the KUMA web interface, under **Resources** → **Storages**, click **Add storage** and edit the settings. In the **ClickHouse cluster nodes** section, specify roles for each server that you are adding: keeper, shard, replica. For more details, see Creating a set of resources for a storage.

         The created resource set for the storage is displayed in the **Resources** → **Storages** section. Now you can create storage services for each ClickHouse cluster node.

      2. To create a storage service, in the KUMA web interface, in the **Resources** → **Active services** section, click **Add service**.

This opens the **Choose a service** window; in that window, select the resource set that you created for the storage at the previous step and click **Create service**. Do the same for each ClickHouse storage.

The number of created services must be the same as the number of nodes in the ClickHouse cluster, for example, 50 services for 50 nodes. The created storage services are displayed in the KUMA web interface in the **Resources** → **Active services** section. Now you need to install storage services on each node of the ClickHouse cluster by using the service ID.

b. On the target computer, create the server part of the storage:

1. In the KUMA web interface, in the **Resources** → **Active services** section, select the storage service that you need and click **Copy ID**.

   The service ID is copied to the clipboard; you need it for running the service installation command.

2. Compose and run the following command on the target computer:

   ```
   sudo /opt/kaspersky/kuma/kuma <storage> --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --
   id <service_ID> --install
   ```

   where:

   - <FQDN> is the fully qualified domain name of the KUMA Core server.
   - <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
   - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

     The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
     You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

     To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

   - <service_ID> is the service ID copied from the KUMA web interface.

   The storage service is installed on the target computer. You can check the status of the service in the web interface under **Resources** → **Active services**.

3. Run the storage service installation command on each target computer listed in the `storage` section of the `expand.inventory.yml` inventory file, one computer at a time. On each computer, the unique service ID within the cluster must be specified in the installation command.

Dedicated keepers are automatically started immediately after installation and are displayed in the **Resources** → **Active services** section with the green status. Services on other storage nodes may not start until services are installed for all nodes in that cluster. Up to that point, services can be displayed with the red status. This is normal behavior when creating a new storage cluster or adding nodes to an existing storage cluster. As soon as the service installation command is run on all nodes of the cluster, all services get the green status.

7. Specify the added servers in the `distributed.inventory.yml` inventory file so that it has up-to-date information in case of a KUMA update.

The extra storage cluster is successfully added.

Migrating the KUMA Core to a new Kubernetes cluster

To migrate KUMA Core to a new Kubernetes cluster:

1. Prepare the k0s.inventory.yml inventory file.

   The kuma_core, kuma_ collector, kuma_correlator, kuma_storage sections of your k0s.inventory.yml inventory file must contain the same hosts that were used when KUMA was upgraded from version 2.1.3 to version 3.0.3 and then to version 3.2, or when a new installation was performed. In the inventory file, set deploy_to_k8s: true, need_transfer: true. Set deploy_example_services: false.

2. Follow the steps for distributed installation using your prepared k0s.inventory.yml inventory file.

Migrating the KUMA Core to a new Kubernetes cluster

When the installer is started with an inventory file, the installer looks for an installed KUMA Core on all hosts where you plan to deploy worker nodes of the cluster. The found Core will be moved from the host to within the newly created Kubernetes cluster.

If the component is not detected on the worker nodes, a clean installation of the KUMA Core is performed in the cluster without migrating resources to it. Existing components must be manually rebuilt with the new Core in the KUMA web interface.

Certificates for collectors, correlators and storages will be re-issued from the inventory file for communication with the Core within the cluster. This does not change the Core URL for components.

On the Core host, the installer does the following:

- Removes systemd services from the host: kuma-core, kuma-vmalert.
- Deletes the internal certificate of the Core.
- Deletes the certificate files of all other components and deletes their records from MongoDB.
- Deletes the following directories:
  - /opt/kaspersky/kuma/core/bin
  - /opt/kaspersky/kuma/core/certificates
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/log
  - /opt/kaspersky/kuma/core/<KUMA Core service ID>/logs
  - /opt/kaspersky/kuma/metrics/<Metrics service ID>/bin
- Migrates data from the Core and its dependencies to a network drive within the Kubernetes cluster.

- On the Core host, it moves the following directories:
  - /opt/kaspersky/kuma/core → /opt/kaspersky/kuma/core.moved
  - /opt/kaspersky/kuma/metrics → /opt/kaspersky/kuma/metrics.moved

After you have verified that the Core was correctly migrated to the cluster, you can delete these directories.

If you encounter problems with the migration, check the logs for records of the 'core-transfer' migration task in the 'kuma' namespace in the cluster (this task is available for 1 hour after the migration).

If you need to perform migration again, you must restore the original names of the /opt/kaspersky/kuma/*.moved directories.

If the /etc/hosts file on the Core host contained lines that were not related to addresses in the 127.X.X.X range, the contents of the /etc/hosts file from the Core host is entered into the coredns ConfigMap when the Core is migrated to the Kubernetes cluster. If the Core is not migrated, the contents of the /etc/hosts file from the host where the primary controller is deployed is entered into the ConfigMap.

Removing a server from a distributed installation

If necessary, you can remove the server from the distributed installation.

To remove a server from a distributed installation:

1. Remove all services from the server that you want to remove from the distributed installation:
2. Remove the servers from the `distributed.inventory.yml` inventory file to make sure the inventory file has up-to-date information in case you need to upgrade KUMA.

The server is removed from the distributed installation.

Deleting a storage cluster

You can remove the storage cluster if necessary.

To remove one or more storage clusters from a distributed installation:

1. Get the ID of the storage service. To do this, in the **Resources** → **Active services** section, open the context menu of the service that you are deleting and click **Copy ID**.
2. Remove the storage service on each cluster server that you want to remove from the distributed installation:
   a. Uninstall the server part of the storage service by running the following command on the target machine:

   ```
   sudo /opt/kaspersky/kuma/kuma <storage> --id <service ID> --uninstall
   ```

   Repeat for each server.

b. Remove the client part of the service in the KUMA web interface in the **Resources** → **Active services** → **Delete** section.

The service is removed.

3. Remove servers from the `storage` section of the `distributed.inventory.yml` inventory file to make sure the inventory file has up-to-date information in case you need to upgrade KUMA or modify its configuration.

The cluster is removed from the distributed installation.

Expanding the Raft cluster

Expanding the Raft cluster in KUMA involves the following steps:

1 Preparing servers for installing KUMA Core services

To prepare servers for installation of additional KUMA Core services:

1. Make sure that you are installing additional KUMA Core services using the same version of the installer that was used to install your current KUMA instance. The full version numbers must be identical.

2. On the control computer, go to the directory containing the extracted installer.

```
cd kuma-ansible-installer
```

3. Depending on the selected activation method, do one of the following:

- Key file.

  Place the `license.key` file in the `<installer directory>/roles/kuma/files/` directory:

  ```
  cp <license>.key <installer_directory>/roles/kuma/files/license.key
  ```

  where:

  - <license> is the name of the key file.

  - <installer_directory> is the installer directory.

- Activation code.

- No action required. Proceed to the next step of the instructions.

4. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

Open the `expand.inventory.yml` inventory file and specify the servers you are adding in the `kuma_core_peers` section. In total, the `kuma_core` and `kuma_core_peers` sections must contain an odd number of servers.

Example of an expand.inventory.yml file for adding servers for additional KUMA Core services

```
kuma:
  vars:
    no_firewall_actions: false
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core_peers:
      hosts:
        kuma-core-4.example.com:
          ip: 0.0.0.0
        kuma-core-5.example.com:
          ip: 0.0.0.0
```

5. On the control computer, run the following command as root from the directory with the unpacked installer:

```
./expand.sh expand.inventory.yml
```

6. Accept the terms of the End User License Agreement.

   If you do not accept the terms of the End User License Agreement, the solution will not be installed.

   Depending on the type of solution activation, the installer produces one of the following results:

   - Key file.

     The servers specified in the `expand.inventory.yml` inventory file are prepared for the installation of additional KUMA Core services.

   - Activation code

     Only the KUMA Core is installed. You will need to activate the solution using an activation code or a key file.

For each target computer specified in the `expand.inventory.yml` inventory file, files required for creating and installing additional KUMA Core services will be added.

2 Creating and installing additional KUMA Core services

To create and install additional KUMA Core services:

1. In the web interface, open the **Resources** → **Active services** section.

2. In the toolbar or menu ⋮, click **Add** and select **Add Core service**.

3. In the panel that opens, enter the name of the KUMA Core and click **Add**.

   The added KUMA Core appears in the services table.

4. In the context menu of the added KUMA Core, select **Copy ID**.

   You can also select the check box next to the added KUMA Core and, in the toolbar or menu (⋮), click **Copy ID**.

   The ID is required to install the KUMA Core on the server.

5. Install KUMA Core on the server. Run the following command on the target computer.

```
sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN>:7210 --pair.fingerprint <CA_cert_ID> --id <service_ID> --install
```

where:

- <FQDN> is the fully qualified domain name of the host from the `kuma_core` section, on which the first KUMA Core service is launched.
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the service ID copied from the KUMA web interface.

Create and install the KUMA Core for each host in the `kuma_core_peers` section. Only one KUMA Core service can be installed on a host.

3 Reflecting the changes in the distributed.inventory.yml inventory file

Add the `kuma_core_peers` section to the `distributed.inventory.yml` inventory file and specify the servers for the additional KUMA Core services that you added to the expand.inventory.yml inventory file. This ensures that the `distributed.inventory.yml` inventory file contains up-to-date information in case you need to update KUMA.

4 Result

Expansion of the Raft cluster is completed. KUMA Core services are added to the Raft cluster and connected to core-1. When installing the resto of the KUMA services, you can specify multiple comma-separated URLs in the installation command to connect to the KUMA Core services in the Raft cluster.

Deleting a Raft cluster node

To delete a Raft cluster node:

1. In the web interface, open the **Resources** → **Active services** section, and in the context menu of the KUMA Core service, select **Copy ID**.

2. In the **Active services** section, select the KUMA Core service installed on the server that you want to remove from the Raft cluster and click **Remove**.

3. Go to the server of the KUMA Core service that you want to remove and stop the service using the following command:

   ```
   sudo systemctl stop kuma-core-<core_ID>.service
   ```

   where:

   <core_ID> is the KUMA Core ID copied from the web interface.

4. Delete the working directory.

   ```
   sudo rmdir <directory_path>
   ```

   where:

   <directory_path> is the full path to the working directory that you want to delete.

5. Remove the systemd service.

The node is deleted from the Raft cluster.

Growing the KUMA Core volume or the Metrics service volume in an active Kubernetes cluster

You may need to grow a volume for the KUMA Core or Metrics service for a KUMA installation in production.

Before increasing the size of volumes, make sure that there is enough free space in the `/opt` directory on the worker nodes of the cluster. You need at least twice as much free space as the planned volume size.

Starting with KUMA 4.0.1, the installer includes the `roles/k0s_prepare/files/k0s-pvc-expand.sh` script, which is copied to the `/root/k0s/` directory on the primary controller of the cluster. This script lets you grow a volume in a production cluster.

Growing a volume using the k0s-pvc-expand.sh script

You can grow a volume in one of the following ways:

- Go to the `/root/k0s/` directory of the master controller and run the `k0s-pvc-expand.sh` script with the `core` or `metrics` option, depending on which volume you want to apply the action to, and specify the new volume size in gigabytes. The volume size must be specified as an integer number without a suffix.
- Manually copy the `k0s-pvc-expand.sh` script to any cluster controller to a directory from which you want to run it and run the script.

```
Example of the command for increasing the size of Metrics service volume to 100 GB
sudo ./k0s-pvc-expand.sh metrics 100
```

```
Example of the command for increasing the size of KUMA Core volume to 200 GB
sudo ./k0s-pvc-expand.sh core 200
```

Script behavior

If the specified volume size is less than or equal to the current size, nothing is done and the script aborts with an error message.

If the new volume size is greater than the current size, the script stops the service that uses the volume (KUMA Core or Metrics). After disconnecting the volume from the pods of the service, the script grows the volume. After resizing the volume, the service is restarted and the expanded volume becomes available to it.

After increasing the volume size, no additional specifications of the volume size in the inventory file are required when upgrading to later versions of KUMA. The KUMA installer will use the current volume sizes and ignore any volume size variables specified in the inventory file that differ from them.

Shrinking the Metrics service volume

Before shrinking the Metrics volume, you need to determine the sufficient volume size based on the metrics in the **Metrics** → **KUMA Metrics service** → **Storage** → **Disk space usage**. Take into account the metrics storage duration and allocate extra disk space if you plan to use additional sources of metrics.

Before shrinking volumes, make sure that no `metrics-transfer-<unique ID>` task exists.

```
k0s kubectl get jobs -n kuma
```

The command should output `"No resources found in kuma namespace."`. The `metrics-transfer` task is automatically deleted 1 hour after completion.

If you want to delete it earlier, you can use the following command:

```
k0s kubectl delete job metrics-transfer -n kuma
```

You can shrink a volume in one of the following ways:

Without data loss

To shrink a Metrics service volume without data loss:

1. Unmount the Metrics service volume:

   a. Get the name of the volume used by the Metrics service:

   ```
   sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
   ```

   You will need this volume name to locate its data and replicas. Replica names begin with the volume name.

   b. Stop the Metrics service:

   ```
   sudo k0s kubectl scale deployment/metrics -n kuma --replicas=0
   ```

   c. Make sure that the `metrics-<UID>` pod of the Metrics service has disappeared (is not present in the command output):

   ```
   sudo k0s kubectl get pods -n kuma
   ```

   d. If the pod does not disappear within a few minutes, force its deletion:

   ```
   sudo k0s kubectl delete pod metrics-<UID> -n kuma --force
   ```

   Use the pod name from the output of the previous command.

   e. Make sure that the Metrics service volume is in the `detached` state:

   ```
   sudo k0s kubectl get volume <volume_name> -n longhorn-system -o json | jq '.status.state'
   ```

2. Create a temporary task:

   a. Create a temporary task named `tmp-metrics-job` in the `kuma` namespace and mount the Metrics service volume:

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: batch/v1
kind: Job
metadata:
  name: tmp-metrics-job
  namespace: kuma
spec:
  ttlSecondsAfterFinished: 300
  backoffLimit: 0
  parallelism: 1
  completions: 1
  template:
    spec:
      containers:
        - name: tmp-container
          image: docker.io/library/busybox:1.35.0
          imagePullPolicy: IfNotPresent
          command: ["/bin/sh"]
          args:
            - -c
            - >-
                sleep 36000
          volumeMounts:
            - mountPath: /metrics
              name: metrics
      restartPolicy: Never
      volumes:
        - name: metrics
          persistentVolumeClaim:
            claimName: metrics
EOF
```

   b. Determine the name of the worker node on which the temporary task is running:

```
sudo k0s kubectl get pods -n kuma -o wide | grep tmp-metrics
```

   c. On this worker node, determine the mount point:

```
sudo lsblk | grep "<volume_name>"
```

   d. Go to the found directory of the `/var/lib/k0s/kubelet/pods/...../mount` type. The content should look like this:

```
ls -al
total 48
drwxrwsr-x 9 root  65532  4096 Aug 26 10:36 .
drwxr-x--- 3 root  root   4096 Aug 26 11:08 ..
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 certificates
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 dashboards
drwxrwsr-x 8 root  65532  4096 Aug 26 10:34 data
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 log
drwxrws--- 2 root  65532 16384 Aug 26 10:34 lost+found
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 rules
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 tmp
```

3. Copy the data:

   a. Copy all data from the `/var/lib/k0s/kubelet/pods/...../mount` directory to a temporary directory, excluding the `lost+found` and `tmp` directories, while preserving the permissions of directories and files.

   b. Go from the mount point to the `/` or `/home` directory to avoid blocking the subsequent volume unmount.

4. Delete the temporary task, pod, PVC, and volume of the Metrics service:

   a. Delete the temporary task with the following command:

```
sudo k0s kubectl delete job tmp-metrics-job -n kuma
```

   b. Make sure that the `metrics-<UID>` pod of the temporary task is not present in the output of the following command:

```
sudo k0s kubectl get pods -n kuma
```

   c. If the pod does not disappear within a few minutes, force its deletion:

```
sudo k0s kubectl delete pod tmp-metrics-job-<UID> -n kuma --force
```

   Use the pod name from the output of the previous command.

   d. Make sure that the Metrics service volume is in the `detached` state:

```
sudo k0s kubectl get volume <volume_name> -n longhorn-system -o json | jq '.status.state'
```

   e. Delete the PVC of the Metrics service:

```
sudo k0s kubectl delete pvc metrics -n kuma
```

   f. Make sure the Metrics service volume is not present in the output of the following command:

```
sudo k0s kubectl get volume <volume_name> -n longhorn-system
```

   On all worker nodes, directories with names beginning with the name of the deleted volume should disappear from the `/opt/longhorn/replicas` directory. If this does not happen, you need to delete them manually.

   > Do not delete replicas belonging to other volumes.

5. Create a new volume:

a. Specify the relevant value in the `storage` string, then create a PVC for the Metrics service:

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: metrics
  namespace: kuma
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: kuma-network-storage
  resources:
    requests:
      storage: 30Gi
EOF
```

b. Get the name of the volume used by the Metrics service again:

```
sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
```

c. Create a temporary task named `tmp-metrics-job` in the `kuma` namespace and mount the new Metrics service volume:

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: batch/v1
kind: Job
metadata:
  name: tmp-metrics-job
  namespace: kuma
spec:
  ttlSecondsAfterFinished: 300
  backoffLimit: 0
  parallelism: 1
  completions: 1
  template:
    spec:
      containers:
        - name: tmp-container
          image: docker.io/library/busybox:1.35.0
          imagePullPolicy: IfNotPresent
          command: ["/bin/sh"]
          args:
            - -c
            - >-
                sleep 36000
          volumeMounts:
            - mountPath: /metrics
              name: metrics
      restartPolicy: Never
      volumes:
        - name: metrics
          persistentVolumeClaim:
            claimName: metrics
EOF
```

d. Determine the name of the worker node on which the temporary task is running:

```
sudo k0s kubectl get pods -n kuma -o wide | grep tmp-metrics
```

e. On this worker node, determine the mount point:

```
sudo lsblk | grep "<volume_name>"
```

f. Go to the found directory of the `/var/lib/k0s/kubelet/pods/...../mount` type.

6. Copy the data:

a. Copy the Metrics service data previously saved in the temporary directory to the located `/var/lib/k0s/kubelet/pods/...../mount` directory, keeping the ownership and permissions of the files. As a result, the contents of the directory should look like this:

```
ls -al
total 48
drwxrwsr-x 9 root  65532  4096 Aug 26 10:36 .
drwxr-x--- 3 root  root   4096 Aug 26 11:08 ..
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 certificates
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 dashboards
drwxrwsr-x 8 root  65532  4096 Aug 26 10:34 data
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 log
drwxrws--- 2 root  65532 16384 Aug 26 10:34 lost+found
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 rules
drwx--S--- 2 65532 65532  4096 Aug 26 10:36 tmp
```

b. Go from the mount point to the `/` or `/home` directory to avoid blocking the subsequent volume unmount.

7. Delete the temporary task and the pod of the temporary task:

a. Delete the temporary task with the following command:

```
sudo k0s kubectl delete job tmp-metrics-job -n kuma
```

b. Make sure that the metrics-<UID> pod of the temporary task is not present in the output of the following command:

```
sudo k0s kubectl get pods -n kuma
```

c. If the pod does not disappear within a few minutes, force its deletion:

```
sudo k0s kubectl delete pod tmp-metrics-job-<UID> -n kuma --force
```

Use the pod name from the output of the previous command.

d. Make sure that the Metrics service volume is in the `detached` state:

```
sudo k0s kubectl get volume <volume_name> -n longhorn-system -o json | jq '.status.state'
```

8. Start the Metrics service.

   a. Run the following command to start the Metrics service with the number of replicas increased to 1:

   ```
   sudo k0s kubectl scale deployment/metrics -n kuma --replicas=1
   ```

   b. Make sure that the Metrics service is running and metrics are available in the web interface.

9. Delete the temporary directory.

The size of the Metrics service volume will be reduced without data loss.

With data loss

To shrink a Metrics service volume with data loss:

1. Get the name of the volume used by the Metrics service:

   ```
   sudo k0s kubectl get pvc metrics -n kuma -o json | jq '.spec.volumeName'
   ```

   You will need this volume name to locate volume data and volume replicas. Replica names begin with the volume name.

2. Stop the Metrics service.

   ```
   sudo k0s kubectl scale deployment/metrics -n kuma --replicas=0
   ```

3. Make sure that the `metrics-<UID>` pod of the Metrics service is not present in the command output:

   ```
   sudo k0s kubectl get pods -n kuma
   ```

4. If the pod does not disappear within a few minutes, force its deletion:

   ```
   sudo k0s kubectl delete pod metrics-<UID> -n kuma --force
   ```

   Use the pod name from the output of the previous command.

5. Make sure that the Metrics service volume is in the `detached` state:

   ```
   sudo k0s kubectl get volume <volume_name> -n longhorn-system -o json | jq '.status.state'
   ```

6. Delete the PVC of the Metrics service:

   ```
   sudo k0s kubectl delete pvc metrics -n kuma
   ```

7. Make sure the Metrics service volume is not present in the output of the following command:

```
sudo k0s kubectl get volume <volume_name> -n longhorn-system
```

On all worker nodes, directories with names beginning with the name of the deleted volume should disappear from the `/opt/longhorn/replicas` directory. If this does not happen, you need to delete them manually.

Do not delete replicas belonging to other volumes.

8. Specify the relevant value in the `storage` string, then create a PVC for the Metrics service.

```
sudo k0s kubectl apply -f - <<EOF
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: metrics
  namespace: kuma
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: kuma-network-storage
  resources:
    requests:
      storage: 30Gi
EOF
```

9. Start the Metrics service, increasing the number of replicas to 1:

```
sudo k0s kubectl scale deployment/metrics -n kuma --replicas=1
```

10. Make sure that the Metrics service is running and metrics are available in the web interface.

The Metrics service volume is successfully shrunk with data loss.

Changing the host name for a single-server deployment

To change the hostname for a single-server installation:

1. Stop all KUMA services by running the following command:

```
sudo systemctl stop kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
```

where:

<service_ID> is the service ID copied from the web interface.

2. Create a recovery file by running the following command:

```
sudo touch /opt/kaspersky/kuma/core/<core_ID>/raft/.reset
```

where:

<core_ID> is the KUMA Core ID copied from the web interface.

3. Go to the systemd directory with the configuration of the KUMA Core service and change the startup parameters:

   - Specify the new FQDN of the host in the `--raft.node.addr` option.
   - Remove the `--raft.join` option if it is specified.

4. On each host where KUMA services are installed (collector, correlator, storage, event router), find the systemd unit file of the corresponding service:

   ```
   systemctl cat kuma-<service_ID>.service
   ```

   where:

   <service_ID> is the service ID copied from the web interface.

   The command returns the directory in which the systemd unit file of the KUMA service is located. Change to this directory and open the unit file for editing.

5. In each unit file of systemd services, change the following settings:

   - For the `--core` option, specify a new name for the host on which the KUMA Core is installed.
   - Specify the new fully qualified name of the machine in the `--advertise.fqdn` option.

6. Apply the new settings by running the following command:

   ```
   sudo systemctl daemon-reload
   ```

7. Change the FQDN of the host in the `/etc/hosts` file. The new FQDN must resolve to the IP address of this host.

8. Change the host name in the operating system:

   ```
   sudo hostnamectl set-hostname <hostname>
   ```

   where:

   <hostname> is the new hostname.

9. Restart the host by running the following command:

   ```
   sudo reboot
   ```

10. After the restart, connect to the host using the new host name.

11. Start the KUMA Core service:

    ```
    sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
    ```

12. Verify that the KUMA web interface is accessible under the new hostname.

13. In the KUMA web interface, go to the **Resources and services** → **Active services** section, and in the list of services, select the check box for the services that you need, then in the toolbar or in the menu (⋮), click **Reset certificate**.

    KUMA automatically generates a new certificate for each service for which the certificate has been reset. You do not need to restart running services, the new certificate is applied automatically. A stopped service must be restarted to have the new certificate applied.

14. Delete the following directories with service certificates by running the following commands:

    ```
    sudo rm -rf /opt/kaspersky/kuma/collector/correlator/storage/eventRouter/<service_ID>/certificates
    sudo rm -rf /opt/kaspersky/kuma/clickhouse/certificates
    ```

    where:

    <service_ID> is the service ID copied from the web interface.

15. In the KUMA web interface, go to the **Resources and services** → **Active services** section, open each active service to manage its settings, and at the **Routing** step, replace the old FQDN with the new FQDN for the destination.

16. Restart all KUMA services:

    ```
    sudo systemctl restart kuma-<collector/correlator/storage/eventRounter/metrics>-<service_ID>.service
    ```

    where:

    <service_ID> is the service ID copied from the web interface.

The KUMA Core host is now running with the new host name, and the services are displayed in the **Resources and services** → **Active services** section with a green status.

Changing the host name for a distributed deployment

To change the hostname on the node on which the KUMA services are installed:

1. Stop all KUMA services except KUMA Core by running the following command:

    ```
    sudo systemctl stop kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
    ```

    where:

    <service_ID> is the service ID copied from the KUMA web interface.

2. Create a recovery file by running the following command:

    ```
    sudo touch /opt/kaspersky/kuma/core/<core_ID>/raft/.reset
    ```

    where:

    <core_ID> is the KUMA Core ID copied from the web interface.

3. Go to the systemd directory with the configuration of the KUMA Core service and change the startup parameters:

   - Specify the new FQDN of the host in the `--raft.node.addr` option.
   - Remove the `--raft.join` option if it is specified.

4. On each host where KUMA services are installed (collector, correlator, storage, event router), find the systemd unit file of the corresponding service:

   ```
   systemctl cat kuma-<service_ID>.service
   ```

   where:

   <service_ID> is the service ID copied from the web interface.

   The command returns the directory in which the systemd unit file of the KUMA service is located. Change to this directory and open the unit file for editing.

5. In each unit file of systemd services, change the following settings:

   - For the `--core` option, specify a new name for the host on which the KUMA Core is installed.
   - Specify the new fully qualified name of the machine in the `--advertise.fqdn` option.

6. Apply the new settings by running the following command:

   ```
   sudo systemctl daemon-reload
   ```

7. Change the FQDN of the host in the `/etc/hosts` file. The new FQDN must resolve to the IP address of this host.

8. Change the host name in the operating system:

   ```
   sudo hostnamectl set-hostname <hostname>
   ```

   where:

   <hostname> is the new hostname.

9. Restart every host on which KUMA services are installed, except for the KUMA Core host, by running the following command:

   ```
   sudo reboot
   ```

10. Restart the KUMA Core host.

    ```
    sudo reboot
    ```

11. In the KUMA web interface, go to the **Resources and services** → **Active services** section, and in the list of services, select the check box for the services that you need, then in the toolbar or in the menu (⋮), click **Reset certificate**.

    KUMA automatically generates a new certificate for each service for which the certificate has been reset. You do not need to restart running services, the new certificate is applied automatically. A stopped service must be restarted to have the new certificate applied.

12. Delete the directories with service certificates by running the following commands:

    ```
    sudo rm -rf /opt/kaspersky/kuma/collector/correlator/storage/eventRouter/<service_ID>/certificates
    sudo rm -rf /opt/kaspersky/kuma/clickhouse/certificates
    ```

    where:

    <service_ID> is the service ID copied from the KUMA web interface.

13. In the KUMA web interface, go to the **Resources and services** → **Active services** section, open each active service to manage its settings, and at the **Routing** step, replace the old FQDN with the new FQDN for the destination.

14. Restart all KUMA services:

    ```
    sudo systemctl restart kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
    ```

    where:

    <service_ID> is the service ID copied from the KUMA web interface.

The KUMA Core host is now running with the new host name, and the services are displayed in the **Resources and services** → **Active services** section with a green status.

Changing the hostname of the KUMA Core

To change the hostname on one of the Raft cluster nodes:

1. Remove the two KUMA Core nodes on which you do not need to change the hostname by doing the following:

   a. In the KUMA web interface, in the **Active services** section, select the KUMA Core service installed on the server that you want to remove from the Raft cluster and click **Remove**.

   b. Go to the server of the KUMA Core service that you want to remove and stop the service:

   ```
   sudo systemctl stop kuma-core-<core_ID>.service
   ```

   where:

   <core_ID> is the KUMA Core service ID copied from the web interface.

   c. Create a backup copy of the working directory.

   d. Delete the working directory:

   ```
   sudo rm -rf /opt/kaspersky/kuma/core/<core_ID>
   ```

e. Delete the systemd service file:

```
sudo rm /usr/lib/systemd/system/kuma-core-<core_ID>.service
```

Repeat the steps to remove the second KUMA Core node.

2. Stop the KUMA Core service on the node on which you want to change the hostname, and disable its autostart by running the following commands:

```
sudo systemctl stop kuma-core-<core_ID>.service
sudo systemctl disable --now kuma-core-<core_ID>
```

3. Change the hostname on the host:

```
sudo hostnamectl set-hostname <hostname>
```

where:

<hostname> is the new hostname.

4. In the `/etc/hosts` file, replace the old hostname with the new one.

5. Restart the node:

```
sudo reboot
```

6. After the node boots, connect to the node under the new hostname.

7. Go to the systemd directory with the configuration of the KUMA Core service and change the startup parameters:

   - Specify the new FQDN of the node in the `--raft.node.addr` option.

   - Remove the `--raft.join` option if it is specified.

8. Apply the new settings:

```
sudo systemctl daemon-reload
```

9. Create a recovery file:

```
sudo -u kuma touch /opt/kaspersky/kuma/core/<core_ID>/raft/.reset
```

10. Configure the KUMA Core autostart:

```
sudo systemctl enable --now kuma-core-<core_ID>
```

11. Start the KUMA Core:

```
sudo systemctl restart kuma-core-<core_ID>.service
```

12. Follow the steps to add the two nodes that you removed at step 1 to the Raft cluster:

    a. In the **Resources** → **Active services** section, click **Add** and in the drop-down list, select **Add Core service**.

    b. This opens the **Add Core service** window; in that window, specify the name of the service in the **Core service name** field and click **Add**. The added service appears in the **Services** list.

    c. Select the check box next to the added KUMA Core service, open the menu in the toolbar , and select **Copy ID**. You will need the ID of the KUMA Core service to install the service on the server.

    d. Run the following command on the target computer.

    ```
    sudo /opt/kaspersky/kuma/kuma core --raft.join <FQDN>:7210 --pair.fingerprint <CA_cert_ID> --id <core_ID> -
    -install
    ```

    where:

    - <FQDN> is the fully qualified domain name of the host from the `kuma_core` section, on which the first KUMA Core service is launched.

    - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

      The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
      You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

      To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

    - <core_ID> is the KUMA Core ID copied from the web interface.

    Repeat the steps to add the other removed node.

Organizing a multi-tenant architecture

KUMA supports *multi-tenant* mode. With this mode, you can create several logically isolated systems (*tenants*) within a single instance of KUMA installed in the infrastructure of the main organization (*main tenant*). These logically isolated systems can be operated by different teams of users. For example, multi-tenancy mode can be used when an organization has several regional offices and the organization's administrator wants to provide KUMA functionality to each office separately. To do this, the administrator creates a tenant for each office. Multi-tenancy is also a useful tool for MSSP providers.

To learn more about working with tenants, watch this video:

https://www.youtube.com/watch?v=nmPxfmRBLI4

Tenants are managed centrally through the KUMA web interface. At the same time, tenants operate independently of each other and have access only to their own resources, services, and settings. Events of tenants are stored separately.

Access to tenants is managed at the user settings level. If there is access to multiple tenants, the user can select which tenants' data is displayed in the sections of the KUMA web interface. The General administrator has access to the data of all tenants.

By default, after installing KUMA, two tenants are created:

- The *Main* (main tenant) contains resources and services that belong to the main tenant. Only a user with the General Administrator role has access to these resources and the ability to deploy services in the Main tenant. The correlator and storage of this tenant get KUMA audit events, user authentication events, and resource creation and modification events. Events of different tenants can be saved in the storage of the Main tenant, and a user has access only to the events of their own tenant. The Main tenant can be renamed, but cannot be deleted.

- The *Shared* (shared tenant) is where the General administrator can place resources, asset categories, and monitoring policies that are available to users of all tenants. For example, correlation rules from the Shared tenant can be connected to the correlators of all tenants. At the same time, the Shared tenant does not contain services, events, or assets.

  Access to a Shared tenant is determined by the role that is assigned to the user. If the user does not have the rights to view or edit the Shared tenant resources, the Shared tenant becomes unavailable for selection in the **Resources** → **<Resource type>** section. The user will not be allowed to export shared resources and resource sets that incorporate resources from the Shared tenant, either through the web interface or through the REST API.

  If any of the services available to the user use shared resources, the names of these resources will be displayed in the service settings, but the user won't have access to view or modify them. The content of active lists is available to the user even if the resource of this active list is shared.

  The limitation does not apply to shared asset categories. Shared resources are also always available to users with the General administrator role.

Cross-tenant interaction rules

Rules for object affiliation to tenants

In KUMA, access to objects and the ability to customize interactions depend on which tenant the created objects (for example, a service or resource) belong to. Therefore, when creating objects, it is important to keep track of which tenant they belong to.

Tenant identification rules:

- The tenant of base events is determined by the collector that processed them.
- The tenant of an object (such as a service or resource) is specified by the user when an object is created.

  Once an object is created, the tenant selected for that object cannot be changed. However, resources can be exported and then imported into another tenant.
- The alert and the correlation event belong to the same tenant as the correlator that created them.

  The tenant name is indicated in the `TenantId` event field.
- If events of different tenants are processed by the same correlator are are not merged, the created correlation events inherit the tenant of the event.
- If the incident is created automatically, it inherits the tenant of the alert. If the incident is created manually, the user can select the tenant.

Examples of cross-tenant interactions

Multitenancy in KUMA provides the capability to centrally investigate alerts and incidents that occur in different tenants. This section includes scenario examples that illustrate which tenants own objects being created.

> When correlating events from different tenants in a common stream, you **should not** group events by tenant. In other words, the `TenantId` event field should not be specified in the **Identical fields** field in correlation rules. Events must be grouped by tenant only if you must not merge events from different tenants.

Correlation of events for one tenant, correlator is allocated for this tenant and deployed at the tenant

Condition:

The collector and correlator are owned by tenant 2 (`tenantID=2`)

Scenario:

1. The collector of tenant 2 receives and forwards events to the correlator of tenant 2.
2. When correlation rules are triggered, the correlator creates correlation events with `tenantID=2`.
3. The correlator forwards the correlation events to the storage partition for tenant 2.

4. An alert is created and linked to the tenant with `tenantID=2`.

5. The events that triggered the alert are appended to the alert.

Result:

- An incident is created manually by the user. The tenant of the incident selected by the user. An alert is linked to an incident either manually or automatically.

- The alert and its linked events can be accessed by employees of tenant 2.

Correlation of events within one tenant with a dedicated correlator deployed on the side of the tenant, whose team will investigate incidents for the tenant.

Condition:

- The collector is deployed at tenant 2 and is owned by this tenant (`tenantID=2`).

- The General administrator determines the tenant of the correlator owner, taking into account which team will investigate incidents of tenant 2: the team of the Main tenant or of tenant 2. The ownership of the alert depends on the ownership of the correlator. Incident ownership depends on the tenant selected by the user when manually creating the incident. If the incident is created automatically, it inherits the tenant of the alert.

Scenario 1. The correlator belongs to tenant 2 (tenantID=2):

1. The collector of tenant 2 receives and forwards events to the correlator.

2. When correlation rules are triggered, the correlator creates correlation events with `tenantID=2`.

3. The correlator forwards the correlation events to the storage partition of tenant 2.

4. An alert is created and linked to the tenant with `tenantID=2`.

5. The events that triggered the alert are appended to the alert.

Result 1:

- The created alert and its linked events can be accessed by employees of tenant 2.

- The alert and its linked events can be accessed by employees of the Main tenant.

Scenario 2. The correlator belongs to the Main tenant (tenantID=1):

1. The collector of tenant 2 receives and forwards events to the correlator.

2. When correlation rules are triggered, the correlator creates correlation events with `tenantID=1`.

3. The correlator forwards the correlation events to the storage partition of the main tenant.

4. An alert is created and linked to the Main tenant with `tenantID=1`.

5. The events that triggered the alert are appended to the alert.

Result 2:

- The alert and its linked events cannot be accessed by employees of tenant 2.
- The alert and its linked events can be accessed by employees of the Main tenant.

Centralized correlation of events received from different tenants

Condition:

- Two collectors are deployed: one at tenant 2 and one at tenant 3. Both collectors forward events to the same correlator.
- The correlator belongs to the Main tenant. A correlation rule waits for events from both tenants.

Scenario:

1. The collector of tenant 2 receives and forwards events to the correlator of the Main tenant.
2. The collector of tenant 3 receives and forwards events to the correlator of the Main tenant.
3. When a correlation rule is triggered, the correlator creates correlation events with `tenantID=1`.
4. The correlator forwards the correlation events to the storage partition of the Main tenant.
5. An alert is created and linked to the Main tenant with `tenantID=1`.
6. The events that triggered the alert are appended to the alert.

Result:

- The alert and its linked events cannot be accessed by employees of tenant 2.
- The alert and its linked events cannot be accessed by employees of tenant 3.
- The alert and its linked events can be accessed by employees of the Main tenant.

The tenant correlates its own events, but the main tenant additionally provides centralized correlation of events.

Condition:

- Two collectors are deployed: in the Main tenant and in tenant 2.
- Two correlators are deployed:
  - Correlator 1 is owned by the Main tenant and receives events from the collector of the Main tenant and correlator 2.
  - Correlator 2 is owned by tenant 2 and receives events from the collector of tenant 2.

Scenario:

1. The collector of tenant 2 receives and forwards events to correlator 2.
2. When a correlation rule is triggered, the correlator of tenant 2 creates correlation events with `tenantID=2`.
   - Correlator 2 forwards the correlation events to the storage partition of tenant 2.
   - Alert 1 is created and linked to the tenant with `tenantID=2`.
   - The events that triggered the alert are appended to the alert.
   - Correlation events from the correlator of tenant 2 are forwarded to correlator 1.
3. The collector of the main tenant receives and forwards events to correlator 1.
4. Correlator 1 processes events of both tenants. When a correlation rule is triggered, correlation events with `tenantID=1` are created.
   - Correlator 1 forwards the correlation events to the storage partition of the Main tenant.
   - Alert 2 is created and linked to the tenant with `tenantID=1`.
   - The events that triggered the alert are appended to the alert.

Result:

- Alert 1 is available to users of tenant 2.
- Alert 2 and its linked events cannot be accessed by employees of tenant 2.
- Alert 2 and its linked events can be accessed by employees of the main tenant.

One correlator for two tenants

> If you do not want events from different tenants to be merged during correlation, you should specify the `TenantId` event field in the **Identical fields** field in correlation rules. In this case, the alert inherits the tenant from the correlator.

Condition:

- Two collectors are deployed: one at tenant 2 and one at tenant 3.
- One correlator owned by the Main tenant (`tenantID=1`) is deployed. It receives events from both tenants but processes them irrespective of each other.

Scenario:

1. The collector of tenant 2 receives and forwards events to the correlator.
2. The collector of tenant 3 receives and forwards events to the correlator.

3. When a correlation rule is triggered, the correlator creates correlation events with `tenantID=1`.

   - The correlator forwards the correlation events to the storage partition of the main tenant.
   - An alert is created and linked to the Main tenant with `tenantID=1`.
   - The events that triggered the alert are appended to the alert.

Result:

- Alerts that were created based on events from tenants 2 and 3 are not available to employees of these tenants.
- Alerts and their linked events can be accessed by employees of the Main tenant.

Example of configuring multi-tenancy

This example describes how to set up multi-tenancy for a holding company that combines companies A, B, and C. At the holding level, a single SOC unit is deployed to serve all companies in the holding. Each company in the holding has its own dedicated employees to ensure information security (hereinafter referred to as "information security employees").

The following requirements must be met:

- SOC employees can manage normalizers and correlation rules that apply to all companies in the holding.
- SOC employees can conduct incident investigations in all companies in the holding.
- Information security employees in companies A and B can manage correlation rules, collectors, and correlators of the respective companies.
- Company C data must not extend beyond the specified perimeter.

To solve this problem, configure multi-tenancy as follows:

1. Create a tenant for each of the companies in the holding: A, B, and C.
2. For each tenant (A, B, and C), create the necessary resources and services, including collectors and correlators managed by the information security employees.
3. Ensure data sovereignty for tenant C:

   a. Create a separate storage for tenant C.

   b. For tenant C, create a correlator destination that sends events to the correlator of tenant C. In the destination configuration window, on the **Services** tab, link the collectors of tenant C.

   c. For tenant C, create a storage destination that will send events to the storage of tenant C. In the destination settings window, on the **Services** tab, link the correlator of tenant C.
4. For the Shared tenant, create the required resources and services, including normalizers and correlation rules that are developed by SOC employees for use in tenants A, B, and C.

5. Configure access rights:

- For SOC employees, create users with roles that provide the following rights:

  - Managing correlation rules and normalizers for the Shared tenant.

    To ensure the specified rights in the role configuration windows for SOC employees, in the list of role permissions in **the Resources** section, select the check boxes next to **the Correlation Rules** and **Normalizers** functional areas, and for each functional area select the **Manage** permission level.

  - Reading events for tenants A, B, and C and managing incident response using all available tools in each tenant.

    To ensure the specified rights in the role configuration windows for SOC employees, do the following in the list of role permissions:

    - Select the check box next to the **Events** section and select the **Read** level of permissions.
    - In the **Incidents** section, select the check box next to the **General** functional area and select the **Manage** level of permissions.
    - Select the check box next to the **Active Directory response** section and select the **Manage** level of permissions.
    - Select the check box next to the **KICS/KATA** section and select the **Manage** level of permissions.
    - Select the check box next to the **KEDR response** section and select the **Manage** level of permissions.

- For information security employees in companies A and B, create users with roles that grant permissions to manage correlation rules, collectors, and correlators for tenants A and B, respectively.

  To ensure the specified rights in the role configuration windows for information security employees in companies A and B, in the list of role permissions in the **Resources** section, select the check boxes next to the **Correlation Rules**, **Collectors**, and **Correlators** functional areas, and for each functional area, select the **Manage** level of permissions.

Working with tenants

This article describes how to navigate to the tenant table, how to create, edit, or delete a tenant, and how to export tenant settings to a CSV file.

> Only users with the General administrator role can create and delete tenants.

Viewing the tenants table

To view the tenants table:

1. In the web interface, open the **Settings** → **Access** → **Tenants** section.
2. If necessary, sort the table by clicking the column header.
3. If you want to find a tenant by name, use the **Search** field.

The resource table contains the following columns:

- **Name** is the name of the tenant.
- **EPS limit** is the EPS (events per second) quota allocated to the tenant out of the overall EPS quota determined by the license.
- **Description** is the description of the tenant.
- **Created**is the tenant creation date.
- **Updated** is the date and time when the tenant information was most recently modified.

Create tenant

To create a tenant:

1. In the web interface, open the **Settings** → **Access** → **Tenants** section.
2. In the toolbar, click **Add**.

   The **Add tenant** window opens.
3. Specify the tenant name in the **Name** field. The name must contain 1 to 128 Unicode characters.
4. If necessary, in the **EPS limit** field, specify the EPS quota for the tenant.

   The sum total of EPS quotas for all tenants must not exceed the EPS available under the license. However, KUMA does not check the values entered in this field.
5. If necessary, fill in the **Description** field. Tenant description may contain no more than 256 Unicode characters.
6. Click **Create**.

The tenant is displayed in the table. For example, to add collectors or correlators to a created tenant, you need to enable the display of this tenant.

Changing a tenant

To edit the tenant:

1. In the web interface, open the **Settings** → **Access** → **Tenants** section.
2. Click the string with the name of the tenant that you want to change.

   Edit tenant window opens.
3. Change the tenant name, EPS limit, or tenant description.
4. Click **Save**.

The tenant parameters are changed.

Deleting a tenant

If a tenant is no longer needed, you can delete it.

> The Main and Shared tenants cannot be deleted.

To delete a tenant:

1. In the web interface, open the **Settings** → **Access** → **Tenants** section.
2. Select the check box next to the tenant that you want to remove, and click **Remove** in the toolbar.
3. In the **Delete tenant?** window that opens, enter the displayed confirmation code and click **OK**.

   The tenant is deleted.

When you delete a tenant, the following happens:

- Services belonging to the tenant, with the exception of agents, are automatically stopped. In the **Resources** → **Active services** section, such services are displayed with a gray status.

  Agent services are not stopped automatically. You can stop the Windows agent services manually in the **Start** → **Services** section. In order to stop the Linux agent services, you can press **`Ctrl`**+**`C`** in the terminal in which the agent was started.
- Reception and processing of events is terminated, and previously received events are deleted.
- All tenant resources are deleted.
- User accounts that have access only to the remote tenant are disabled—active sessions are terminated, and an error message is displayed when attempting to log in again.
- In the **Settings** → **Access** → **Domain authentication** section, under **Administration groups**, the role filters created for this tenant get deleted.

Exporting tenant parameters

To export tenant parameters:

1. In the web interface, open the **Settings** → **Access** → **Tenants** section.
2. In the toolbar, click **Export** and select one of the following options:
   - **All fields**.

     It is recommended to select this option if you want to save all tenant parameters to a file, for example, for maintaining internal documentation. The file contains the following fields: `id`, `name`, `description`, `main`, `eps`, `epsLimit`, `createdAt`, `updatedAt`.

- **For a dictionary**.

  It is recommended to select this option, for example, to configure event enrichment. In this case, the file contains the fields `id` and `name`.

The tenant parameters are saved to a CSV file.

Enabling and disabling the display of tenants

If you have access to multiple tenants, using Kaspersky SIEM you can select data of which tenants will be displayed in the web interface. This determines which tenants can be specified, for example, when creating resources, services, layouts, report templates, widgets, incidents, or Kaspersky SIEM assets, where you need to select a tenant.

To enable or disable tenant display:

1. In the main menu of the web interface, click **Selected tenants**.

   The tenant selection area opens.

2. Select or clear the check boxes next to the tenants you want to enable or disable.

   At least one tenant must be selected for display.

   You can use the **Search** field to search for tenants.

3. Close the tenant selection area by clicking **Selected tenants** or the X icon.

Sections of the web interface display only the data and analytics related to the selected tenants.

Managing Users and Configuring Access by Roles

It is possible for multiple users to have access to KUMA. Users are assigned user roles, which affect the tasks the users can perform. The same user may have different roles for different tenants. However, you cannot assign roles to yourself, even if your user account has the General administrator role; the displayed list of roles cannot be edited.

You can create or edit user accounts in the **Settings** → **Users** section of the KUMA web interface. Users are also created automatically in the application if KUMA integration with Active Directory is enabled and the user is logging in to the KUMA web interface for the first time using their domain account.

All internal users whose accounts were created in the KUMA web interface, except for the admin account, must change their password when they first log into the KUMA web interface. Subsequently, these users must regularly change their password in accordance with corporate policies, but at least once every three months.

User accounts are displayed in the **Users** window of the KUMA web interface on the **Active users** and **Inactive users** tabs, depending on the user account status, *Active* or *Inactive*. You can use the **Search** field to look for users. You can sort the tables by clicking the column header and selecting **Ascending** or **Descending**.

You can create, edit, or disable user accounts. When editing user accounts (your own or the accounts of others), you can generate an API token for them.

To disable a user account:

In the **Settings** → **Access** → **Users** → **Active users** section of the KUMA web interface, select the check box next to the relevant user and click **Disable**.

User roles

A user's access to KUMA functionality depends on the user's role. A role is a set of rights and permissions to manage the solution. KUMA uses predefined roles with certain sets of access rights, as well as custom roles.

Predefined roles

When installing KUMA, the following predefined roles are created by default:

- The *General administrator* role is for users responsible for the functioning of KUMA components. For example, they install KUMA components, monitor the performance of services within these components, create backups, and add users. These users have full access to KUMA.
- The *Tenant administrator* role is for users responsible for the functioning of KUMA components owned by a specific tenant.
- The *Tier 2 analyst* role is for users responsible for configuring the KUMA system to receive and process events of a tenant. They also create and tweak correlation rules.
- The *Tier 1 analyst* role is for users responsible for configuring the KUMA system to receive and process events of a tenant. They also create and tweak correlation rules. Users with this role have fewer privileges than Tier 2 analysts.
- *Junior analyst*—this role is for users dealing with immediate security threats of a specific tenant. A user with this role can check resources of the Shared tenant through the REST API.
- The *Interaction with NCIRCC* role can be selected if the license includes the GosSOPKA module. Users with this role receive notifications by default.
- The *Interaction with CII* role can be selected if the license includes the GosSOPKA module. Users with this role receive notifications by default.
- *Access to shared resources*—this role is intended for managing the Shared tenant. Users with this role have read access to shared resources.
- *Manage shared resources*—this role is intended for managing the Shared tenant. Users with this role have edit access to shared resources.

> The Interaction with NCIRCC and Interaction with CII roles are displayed only if your license covers the GosSOPKA module.

Each predefined role has the rights to perform certain actions in KUMA.

Custom roles

If existing predefined roles are inadequate for a user, you can create and use your own unique sets of rights and permissions by setting up custom roles.

In the **Settings** → **Access** → **Roles** section, you can perform the following actions:

- Creating custom roles, including by cloning existing roles (including predefined roles)
- Managing the settings of custom roles
- Viewing the set of rights and permissions of a role, the list of users with the selected role, as well as tenants of user roles
- Deleting custom roles

Rights of predefined roles

In KUMA, permissions are assigned to predefined user roles with regard to sections of the solution. Information about user permissions in various sections is given in the tables below.

User permissions for the Reports section

The Reports section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Create report template	yes	yes	yes	yes	no	no	no	no	no
View and edit templates and reports	yes	yes	yes	yes	no	no	no	no	no
Generate reports	yes	yes	yes	yes	no	no	no	no	no
View generated reports	yes	yes	yes	yes	yes	no	no	no	no
Modify generated reports	yes	yes	yes	yes	no	no	no	no	no
Export generated reports	yes	yes	yes	yes	yes	no	no	no	no
Delete templates and generated reports	yes	yes	yes	yes	no	no	no	no	no
Manage report generation settings	yes	yes	yes	yes	no	no	no	no	no

Duplicate report template	yes	yes	yes	yes	no	no	no	no	no
Open the generated report by email	yes	yes	yes	yes	yes	no	no	no	no

User permissions for the Dashboard section

The Dashboard section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View data on the dashboard and change layouts	yes	yes	yes	yes	yes	no	no	yes	yes
View the Universal layout	yes	yes	yes	yes	yes	no	no	yes	yes
Add layouts	yes	yes	yes	yes	no	no	no	no	no
Edit and rename layouts	yes	yes	yes	yes	no	no	no	no	no
Delete layouts	yes	yes	yes	yes	no	no	no	no	no
Enable and disable the TV mode	yes	yes	yes	yes	yes	no	no	yes	yes

User permissions for the Resources section

The Resources → Services & Resources → Services → Active services section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of active services	yes	yes	yes	yes	yes	no	no	yes	yes
View and delete partitions in storage	yes	no	no	no	no	no	no	no	no
Download service logs	yes	yes	yes	yes	yes	no	no	yes	yes
Copy the service ID	yes	yes	yes	yes	yes	no	no	yes	yes
Refresh the table of active services	yes	yes	yes	yes	yes	no	no	yes	yes
Go to Events	yes	yes	yes	yes	yes	no	no	yes	yes
View the contents of the active list	yes	yes	yes	yes	no	no	no	no	no
View the content of a context table	yes	yes	yes	yes	no	no	no	no	no
Import/export/clear/add/edit/delete active list content	yes	yes	yes	yes	no	no	no	no	no
Import/export/clear/add/edit/delete context table content	yes	yes	yes	yes	no	no	no	no	no
Create a set of resources for services	yes	yes	yes	no	no	no	no	no	no
Create a service under Resources → Services → Active services	yes	yes	no	no	no	no	no	no	no

Delete services	yes	yes	no	no	no	no	no	no	no
View services that have the gray status	yes	no	no	no	no	no	no	no	no
Restart services	yes	yes	no	no	no	no	no	no	no
Update the settings of services	yes	yes	yes	no	no	no	no	no	no
Reset certificates	yes	yes	no	no	no	no	no	no	no

User permissions for the Data mining section

The Data mining section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the scheduler configuration	yes	yes	yes	no	no	no	yes	no	no
Create a scheduler	yes	yes	yes	no	no	no	no	no	no
Link storages and correlators	yes	yes	yes	no	no	no	no	no	no
Run	yes	yes	yes	no	no	yes	no	no	no

User permissions for the Resources configuration and Services configuration sections

The Resources → Resources configuration and Configuring services and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of resource and service configurations	yes	yes	yes	yes	no	yes	yes	no	no
Create a service configuration	yes	yes	yes	yes	no	no	no	no	no
Create a resource configuration	yes	yes	yes	yes	no	yes	no	no	no
Duplicate the configuration of a resource/service	yes	yes	yes	yes	no	yes	no	no	no
Edit the configuration of a resource/service	yes	yes	yes	yes	no	yes	no	no	no
Delete the configuration of a resource/service	yes	yes	yes	yes	no	yes	no	no	no
Import the configuration of a resource/service from a file	yes	yes	yes	yes	no	yes	no	no	no
View the repository, import the resources from the repository	yes	yes	yes	no	no	no	no	no	no
Export the configuration of a resource/service	yes	yes	yes	yes	no	yes	yes	no	no
Export correlation rules to MITRE ATT&CK Navigator	yes	yes	yes	yes	no	no	no	no	no

Create and edit a resource configuration in the Shared tenant	yes	no	no	no	no	yes	yes	no	no
View a resource in the Shared tenant (including linking, export, duplication)	yes	no	no	no	no	yes	yes	no	no

User permissions for the List of event sources section

The Source status → List of event sources section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View sources of events	yes	yes	yes	yes	yes	yes	no	yes	yes
Change sources of events	yes	yes	yes	no	no	yes	no	no	no
Delete sources of events	yes	yes	yes	no	no	yes	no	no	no

User permissions for the Monitoring policies section

The Source status → Monitoring policies section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View monitoring policies	yes	yes	yes	yes	yes	yes	yes	yes	yes
Create monitoring policies	yes	yes	yes	no	no	yes	no	no	no
Edit monitoring policies	yes	yes	yes	no	no	yes	no	no	no
Delete monitoring policies	yes	yes	yes	no	no	yes	no	no	no

User permissions for the Assets section

The Assets section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Assets									
View the list of assets	yes	yes	yes	yes	yes	no	no	yes	yes
View the list of categories	yes	yes	yes	yes	yes	yes	yes	yes	yes
Add/edit/delete asset categories	yes	yes	yes	yes	no	no	no	no	no
Add asset categories in the Shared tenant	yes	no	no	no	no	no	no	no	no

Link assets to an asset category of the Shared tenant	yes	yes	yes	yes	no	yes	yes	no	no
Add assets	yes	yes	yes	yes	no	no	no	no	no
Edit assets	yes	yes	yes	yes	no	no	no	no	no
Delete assets	yes	yes	yes	yes	no	no	no	no	no
Import assets from Kaspersky Security Center	yes	yes	yes	yes	no	no	no	no	no
Start tasks on assets in Kaspersky Security Center	yes	yes	yes	yes	no	no	no	no	no
Run tasks to move an asset to a Kaspersky Security Center administration group	yes	yes	yes	yes	no	no	no	no	no
Run tasks on assets in Kaspersky Endpoint Detection and Response	yes	yes	yes	yes	no	no	no	no	no
Initiating the change of asset status in KICS for Networks	yes	yes	yes	yes	no	no	no	no	no
Confirm updates to fix the asset vulnerabilities and accept the licensing agreements	yes	yes	no	no	no	no	no	no	no
Editing CII categorization in the asset card	yes	no	no	no	no	no	no	no	yes
Editing custom fields of assets (**Settings** → **Other** → **Assets**)	yes	yes	yes	yes	no	no	no	no	no

User permissions for the Alerts section

The Alerts section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Change the severity of alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Open the details of alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Assign responsible users	yes	yes	yes	yes	yes	no	no	yes	yes
Close alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Add comments to alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Attach an event to alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Detach an event from alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Edit and delete someone else's filters	yes	yes	no	no	no	no	no	no	no

User permissions for the Incidents section

The Incidents section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Create blank incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Manually create incidents from alerts	yes	yes	yes	yes	yes	no	no	yes	yes
Change the severity of incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Open the incident details	yes	yes	yes	yes	yes	no	no	yes	yes
Assign executors	yes	yes	yes	yes	yes	no	no	yes	yes
Close incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Add comments to incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Attach alerts to incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Detach alerts from incidents	yes	yes	yes	yes	yes	no	no	yes	yes
Edit and delete someone else's filters	yes	yes	no	no	no	no	no	no	no
Export incidents to RuCERT	yes	no	no	no	no	no	no	yes	no
Send files to NCIRCC	yes	no	no	no	no	no	no	yes	no
Download files sent to NCIRCC	yes	no	no	no	no	no	no	yes	no
Export additional incident data to NCIRCC upon request	yes	no	no	no	no	no	no	yes	no
Send messages to NCIRCC	yes	no	no	no	no	no	no	yes	no
View messages from NCIRCC	yes	no	no	no	no	no	no	yes	no
View incident data exported to NCIRCC	yes	no	no	no	no	no	no	yes	no

User permissions for the Events section

The Events section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of events	yes	yes	yes	yes	yes	no	no	yes	yes

Search events	yes	yes	yes	yes	yes	no	no	yes	yes
Open the details of events	yes	yes	yes	yes	yes	no	no	yes	yes
Open statistics	yes	yes	yes	yes	yes	no	no	yes	yes
Perform a retrospective scan	yes	yes	yes	no	no	no	no	no	no
Export events to a TSV file	yes	yes	yes	yes	yes	no	no	yes	yes
View filters (search query)	yes	yes	yes	yes	yes	yes	yes	yes	yes
Add (save) filter	yes	yes	yes	yes	yes	yes	no	yes	yes
Edit or delete someone else's filter folders	yes	yes	no	no	no	no	no	no	no
Delete own filters	yes	yes	yes	yes	yes	yes	no	yes	yes
Delete other users' filters	yes	yes	no	no	no	no	no	no	no
Start ktl enrichment	yes	yes	yes	yes	no	no	no	no	no
Run tasks on Kaspersky Endpoint Detection and Response assets in event details	yes	yes	yes	yes	no	no	no	no	no
Create presets	yes	yes	yes	yes	yes	yes	no	yes	yes
Delete presets	yes	yes	yes	yes	yes	yes	no	yes	yes
View and use presets	yes	yes	yes	yes	yes	yes	yes	yes	yes
Run queries in the background	yes	yes	yes	yes	yes	no	no	yes	yes

User permissions for the Users and actions section

The Settings → Access → Users section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of users	yes	no	no	no	no	no	no	no	no
Add a user	yes	no	no	no	no	no	no	no	no
Edit a user	yes	no	no	no	no	no	no	no	no
Generate token	yes	yes	yes	yes	yes	yes	yes	yes	yes
Change access rights for a token	yes	yes	yes	yes	yes	yes	yes	yes	yes
View the data of their own profile	yes	yes	yes	yes	yes	yes	yes	yes	yes
Edit the data of their own profile	yes	yes	yes	yes	yes	yes	yes	yes	yes

User permissions for the LDAP server section

The Settings → Integrations → LDAP server section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the LDAP connection settings	yes	yes	yes	yes	no	no	no	no	no
Edit the LDAP connection settings	yes	yes	no	no	no	no	no	no	no
Delete the configuration of an entire tenant from the settings	yes	yes	no	no	no	no	no	no	no
Import assets	yes	yes	no	no	no	no	no	no	no

User permissions for the Tenants section

The Settings → Access → Tenants section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of tenants	yes	no	no	no	no	no	no	no	no
Add tenants	yes	no	no	no	no	no	no	no	no
Change tenants	yes	no	no	no	no	no	no	no	no
Export tenants	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the "Domain authentication" section

The "Settings → Access → Domain authentication" section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the Active Directory connection settings	yes	no	no	no	no	no	no	no	no
Edit the Active Directory connection settings	yes	no	no	no	no	no	no	no	no
Add filters based on roles for tenants	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the General section

The Settings → Other → General section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the SMTP connection settings	yes	no	no	no	no	no	no	no	no
Edit the SMTP connection settings	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the License section

The Settings → Other → License section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of added license keys	yes	no	no	no	no	no	no	no	no
Add license keys	yes	no	no	no	no	no	no	no	no
Delete license keys	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the Kaspersky Security Center section

The Settings → Integrations → Kaspersky Security Center section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of successfully integrated Kaspersky Security Center servers	yes	yes	yes	yes	no	no	no	no	no
Add Kaspersky Security Center connections	yes	yes	no	no	no	no	no	no	no
Delete Kaspersky Security Center connections	yes	yes	no	no	no	no	no	no	no
Delete the configuration of an entire tenant from the settings	yes	yes	no	no	no	no	no	no	no
Start the tasks for importing Kaspersky Security Center assets	yes	yes	no	no	no	no	no	no	no

User permissions for the KICS/KATA section

The Settings → Integrations → KICS/KATA section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View a list of KICS/KATA servers with which integration has been configured	yes	yes	no	no	no	no	no	no	no
Add and modify the settings of KICS/KATA integration	yes	yes	no	no	no	no	no	no	no
Delete the settings of KICS/KATA integration	yes	yes	no	no	no	no	no	no	no
Run the tasks to import assets from the KICS/KATA settings	yes	yes	no	no	no	no	no	no	no

User permissions for the Kaspersky Automated Security Awareness Platform section

The Settings → Integrations → Kaspersky Automated Security Awareness Platform section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the ASAP integration settings	yes	no	no	no	no	no	no	no	no
Edit the ASAP integration settings	yes	no	no	no	no	no	no	no	no

User permissions for the Kaspersky Endpoint Detection and Response section

The Settings → Integrations → Kaspersky Endpoint Detection and Response section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the connection settings	yes	yes	yes	yes	no	no	no	no	no
Add, edit and disconnect the connections when the distributed solution mode is enabled	yes	no	no	no	no	no	no	no	no
Enable the distributed solution mode	yes	no	no	no	no	no	no	no	no
Add connections when the distributed solution mode is disabled	yes	yes	no	no	no	no	no	no	no
Delete the connections when the distributed solution mode is disabled	yes	yes	no	no	no	no	no	no	no
Delete the configuration of an entire tenant from the settings	yes	yes	no	no	no	no	no	no	no

User permissions for the Kaspersky CyberTrace section

The Settings → Integrations → Kaspersky CyberTrace section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the CyberTrace integration settings	yes	no	no	no	no	no	no	no	no
Edit the CyberTrace integration settings	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the IRP / SOAR section

The Settings → Integrations → IRP / SOAR section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the settings for integration with IRP / SOAR	yes	no	no	no	no	no	no	no	no
Edit the IRP/SOAR integration settings	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the Kaspersky Threat Lookup section

The Settings → Integrations → Kaspersky Threat Lookup section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the Threat Lookup integration settings	yes	no	no	no	no	no	no	no	no
Edit the Threat Lookup integration settings	yes	no	no	no	no	no	no	no	no

This section is available only to the general administrator.

User permissions for the Alerts section

The Settings → Other → Alerts section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the parameters	yes	yes	yes	yes	no	no	no	no	no

Edit the parameters	yes	yes	yes	no	no	no	no	no	no
Delete the configuration of an entire tenant from the settings	yes	yes	yes	no	no	no	no	no	no

User permissions for the Automatic linking of alerts to incidents section

The Settings → Other → Incidents → Automatic linking of alerts to incidents section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the parameters	yes	yes	yes	yes	no	no	no	no	no
Edit the parameters	yes	no	no	no	no	no	no	no	no

This section is available for an account with the Tenant administrator, Tier 2 analyst, or Tier 1 analyst role if the role is assigned in the Main tenant.

User permissions for the Incident types section

The Settings → Other → Incidents → Incident types section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the categories reference	yes	yes	yes	yes	no	no	no	no	no
View the categories charts	yes	yes	yes	yes	no	no	no	no	no
Add categories	yes	yes	no	no	no	no	no	no	no
Edit categories	yes	yes	no	no	no	no	no	no	no
Delete categories	yes	yes	no	no	no	no	no	no	no

User permissions for the NCIRCC section

The Settings → Integrations → NCIRCC section and actions in this section	General administrator	Tenant administrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the parameters	yes	no	no	no	no	no	no	no	no
Edit the parameters	yes	no	no	no	no	no	no	no	no

User permissions for the Asset audit section

The Settings → Other → Assets → Asset audit section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Create, clone and edit the settings	yes	yes	yes	no	no	no	no	no	no
View the parameters	yes	yes	yes	yes	no	no	no	no	no
Delete settings	yes	yes	yes	no	no	no	no	no	no

User permissions for the Repository update section

The Settings → Other → Repository update section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the parameters	yes	yes	yes	no	no	no	no	no	no
Edit the parameters	yes	no	no	no	no	no	no	no	no
Start the repository update task manually	yes	yes	yes	no	no	no	no	no	no

User permissions for the Assets section

The Settings → Other → Assets section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Add, edit, and delete the asset fields	yes	no	no	no	no	no	no	no	no

User permissions for the Access to spaces section

The Settings → Access → Access to spaces section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Viewing the list of sets	yes	no	no	no	no	no	no	no	no
Adding, editing, deleting a space set	yes	no	no	no	no	no	no	no	no
Setting the default space set	yes	no	no	no	no	no	no	no	no
Assigning a space set to a user	yes	no	no	no	no	no	no	no	no

User permissions for the Tags section

The Settings → Other → Tags section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View the list of tags	yes	yes	yes	yes	no	no	no	no	no

User permissions for the Extended event schema fields scheme

The Options → Other → Extended event schema fields section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Viewing the table of extended event schema fields	yes	yes	yes	yes	yes	no	yes	no	no
Exporting extended event schema fields	yes	yes	yes	yes	yes	no	yes	no	no
Adding and modifying extended event schema fields	yes	yes	yes	yes	yes	no	no	no	no
Importing extended event schema fields	yes	yes	yes	yes	yes	no	no	no	no
Removing and disabling extended event schema fields	yes	no	no	no	no	no	no	no	no

User permissions for the Metrics section

The Metrics section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Open metrics	yes	no	no	no	no	no	no	no	no

User permissions for the Task manager section

The Task manager section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
View a list of your own tasks	yes	yes	yes	yes	yes	no	no	yes	yes
Finish your own tasks	yes	yes	yes	yes	yes	no	no	yes	yes
Restart your own tasks	yes	yes	yes	yes	yes	no	no	yes	yes
View a list of all tasks	yes	yes	yes	yes	yes	no	no	yes	yes

Finish any task	yes	no	no	no	no	no	no	no	no
Restart any task	yes	yes	yes	yes	yes	no	no	yes	yes
Restart tasks of the Run query in the background type	yes	yes	yes	yes	yes	no	no	yes	yes
Stop tasks of the "Run query in the background" type, and initiate the execution of a query in the **Events** section	yes	yes	yes	yes	yes	no	no	yes	yes

User permissions for the CyberTrace section

The CyberTrace section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Open the section	yes	no	no	no	no	no	no	no	no

This section is not displayed in the web interface unless CyberTrace integration is configured under **Settings** → **Integrations** → **Kaspersky CyberTrace**.

User permissions for the Access to tenant data section

The Access to tenant data section and actions in this section	General admin-istrator	Tenant admin-istrator	Tier 2 analyst	Tier 1 analyst	Junior analyst	Manage shared resources	Read shared resources	Interaction with NCIRCC	Access to CII
Access to tenants	yes	yes	yes	yes	yes	no	no	yes	yes
Shared tenant	yes	yes	yes	yes	yes	yes	yes	yes	yes
Main tenant	yes	yes	yes	yes	yes	no	no	yes	yes

Creating a user role

When you create a user role, you can give this role permissions to create users and manage roles. Users with such a role can create another user account for themselves or a role with broad rights and permissions (including administrative control). We strongly recommend that you only assign administrator rights to trusted users.

In KUMA 4.6, you cannot create a custom role with access to the Shared tenant and its resources. For users needing access to the Shared tenant, assign Shared tenant roles. By default, access to the Shared tenant is granted to the General administrator and to roles that have the following permissions: manage shared resources, read shared resources, and access to shared dashboards.

To create a custom role:

1. In the KUMA web interface, in the **Settings** → **Access** → **Roles** section, click the **New** button.

   The role is created in an enabled state. You can disable it in the table of roles or in the sidebar with the description of role settings.

2. In the **Name** field, specify the name of a user role. The name must contain 1 to 128 Unicode characters.

3. If necessary, fill in the **Description** field (maximum 4000 characters).

4. In the **List of permissions** settings section, select the check boxes next to the functional areas available for the created role.

   The list of functional areas includes individual functional areas and groups of functional areas. For example, the **KSC** group includes the **General** (viewing the status of Kaspersky Security Center tasks) and **Updates** (reading Kaspersky Security Center updates) functional areas. You can select an entire group of functional areas or individual functional areas from a group.

5. For the selected functional areas, specify the level of rights and permissions.

   By default, when a role is created, the functional area is assigned with the same permission level as the predefined Junior analyst role.

   > AI-related functional areas are displayed in a role if the AI module is available under the license. Functional areas related to NKTsKI and KII are displayed if the GosSOPKA module is available under the license.

   The following permissions are available in KUMA:

   - **No rights** does not grant any permissions to manage objects.
   - **Read Read** grants read permissions.
   - **Manage created Manage created** grants full user permissions in the functional area (reading and duplicating all objects, modifying and deleting own objects) for objects created by the user.
   - **Manage Manage** grants full management permissions for the functional area (read, create, edit, delete).

   Only one permission level may be specified per functional area.

   You can specify the permissions as follows:

   - Specify the rights in the **Permissions** column separately for each selected functional area.
   - Select all functional areas included in the group, or all functional areas, and specify the rights using the buttons above the table.

     If you assign permissions using the buttons above the table, the permissions are assigned only to those functional areas to which they are available. For example, you can set **No rights** or **Read** permissions for the **Events** functional area. If you select the **Manage** level of permissions for the selected functional areas or groups of functional areas using the button above the table, the level of permissions is only changed for those functional areas to which the **Manage** permission is available. For the **Events** functional area, for which this permission is not available, the permission is not changed.

6. Then click the **Create** button.

The created role is displayed in the table of roles that can be assigned to the user.

Creating a custom role based on an existing one

You can create a custom role by copying an existing one (including a predefined role).

To create a role based on an existing role:

1. In the **Settings** → **Access** → **Roles** section of the KUMA web interface, use a check box to select the role whose settings you want to duplicate.

2. In the toolbar, click the **Duplicate** button.

3. In the **Create role** window that opens, change the required settings.

4. Then click the **Create** button.

   The new role with the **Enabled** status is displayed in the table of roles.

Example of creating a role based on an existing one

Information security employee of the organization works under an account with the Level 1 Analyst role. The information security employee's operational tasks also require the right to restart collector and agent services.

To assign an information security employee the rights to restart collectors and agents:

1. Create a custom role that combines the rights of the Level 1 Analyst role with the rights to manage collectors and agents.

   a. In the KUMA web interface, in the **Settings** → **Access** → **Roles** section, select the check box next to the **Tier 1 Analyst** role.

   b. In the toolbar, click the **Duplicate** button.

      This opens the **Create role** window.

   c. In the **Name** field, enter the name of a new role.

   d. In the **list of permissions** for the group of functional areas in the **Services** section, select the check box next to the **Service restart** functional area and select the **Manage** level of permissions.

   e. Then click the **Create** button.

   The new role with the **Enabled** status is displayed in the table of roles.

2. For the account under which the information security employee works, add the role that was created in the previous steps.

Functional areas and permissions available to them

The following table lists KUMA functional area groups and the functional areas that they include. For each functional area, a description is given as well as a list of available authorization levels that can be set for custom roles.

Groups of functional areas and the functional areas in them

Functional area	Description	Possible permissions
Group of functional areas: Alerts		
Alerts	Working with alerts	• Manage • Read • No rights
Group of functional areas: Incidents		
Common	Working with incidents	• Manage • Read • No rights
Types	Managing incident types	• Manage • No rights
NCIRCC	Exporting incidents to RuCERT	• Manage • No rights
Group of functional areas: Events		
Events	Searching events	• Read • No rights
Group of functional areas: Response		
Adding an indicator to the list of indicators of compromise	Adding an indicator to the list of excluded CyberTrace indicators of compromise from the event card (manually)	• Manage • No rights
KATA	Response using KATA means	• Manage • No rights
KICS	Response using KICS means	• Manage • No rights
KSC	Response using KSC means	• Manage • Read • No rights
Active Directory	Response using Active Directory means	• Manage • No rights
KASAP	Move between KASAP groups	• Manage • Read • No rights
Group of functional areas: Assets		
Common	Managing assets	• Manage • Read • No rights
Asset categorization	Managing automatic asset categorization rules	• Manage • Read • No rights
Categorize CII assets	Read and edit settings when categorizing a CII asset in the asset card	• Manage • No rights

Functional area	Description	Possible permissions
Group of functional areas: Resources		
Collectors	Managing collector configuration	• Manage • Manage created • Read • No rights
Correlators	Managing correlator configuration	• Manage • Manage created • Read • No rights
Storages	Managing storage configuration	• Manage • Manage created • Read • No rights
Agents	Managing agent configuration	• Manage • Manage created • Read • No rights
Event routers	Managing event router configuration	• Manage • Manage created • Read • No rights
Normalizers	Managing normalizer configuration	• Manage • Manage created • Read • No rights
Connectors	Managing connector configuration	• Manage • Manage created • Read • No rights
Destinations	Managing destination configuration	• Manage • Manage created • Read • No rights
Filters	Managing filter configuration	• Manage • Manage created • Read • No rights
Active list	Managing active list configuration	• Manage • Manage created • Read • No rights
Context tables	Managing the configuration of context tables	• Manage • Manage created • Read • No rights
Dictionaries	Managing dictionary configuration	• Manage • Manage created • Read • No rights
Proxies	Managing proxy server configuration	• Manage • Manage created

Functional area	Description	Possible permissions
		• Read • No rights
Secrets	Managing secret configuration	• Manage • Manage created • Read • No rights
Notification templates	Managing notification template configuration	• Manage • Manage created • Read • No rights
Aggregation rules	Managing aggregation rule configuration	• Manage • Manage created • Read • No rights
Correlation rules	Managing correlation rule configuration	• Manage • Manage created • Read • No rights
Enrichment rules	Managing enrichment rule configuration	• Manage • Manage created • Read • No rights
Response rules	Managing response rule configuration	• Manage • Manage created • Read • No rights
Data collection and analysis rules	Managing data collection and analysis rules	• Manage • Manage created • Read • No rights
Segmentation rules	Managing segmentation rule configuration	• Manage • Manage created • Read • No rights
Dashboards	Managing dashboards	• Manage • Manage created • Read • No rights
Report templates	Managing report templates	• Manage • Manage created • Read • Read created • No rights
Importing resources	Importing any resources, folders, and asset categories, including overwriting existing ones	• Manage • No rights
Exporting resources	Exporting any resources, folders, and asset categories	• Read • No rights
Import from repository	Importing resources from a repository	• Manage • No rights
Repository	Reading resource repository	• Read • No rights
Directories	Managing directories	• Manage • Manage

Functional area	Description	Possible permissions
		created • Read • No rights
Field sets	Managing user-created field sets	• Manage • Manage created • Read • No rights
Panels of secrets	Viewing the panel of secrets in the **Resources** section	• Read • No rights
Group of functional areas: Creating exclusions from correlation rules		
Create exclusions	Creating exclusions from correlation rules	• Manage • No rights
Read and delete exclusions	Managing exclusions from correlation rules	• Manage • No rights
Group of functional areas: Active services		
Subgroup: Work with services		
Collector	Managing collector service	• Manage • Read • No rights
Correlator	Managing correlator service	• Manage • Read • No rights
Active lists on correlator	Managing the content of active list and context table on correlator	• Manage • Read • No rights
Repository	Managing storage service	• Manage • Read • No rights
Storage partitions	Managing storage partitions in active services	• Manage • Read • No rights
Active queries to ClickHouse	Managing active queries to ClickHouse	• Manage • Read • No rights
Agent	Managing agent service	• Manage • Read • No rights
Core	Managing core service	• Manage • Read • No rights
Event router	Managing event router service	• Manage • Read • No rights
Subgroup: Actions		
Updating configuration	Updating active service configuration	• Manage • No rights
Restart	Restart an active service	• Manage • No rights
Reset certificate	Resetting active service certificate	• Manage • No rights
Download active service artifacts	Download active service artifacts	• Manage • No rights
Remaining services from deleted tenants	Reading and deleting services left behind by deleted tenants	• Manage • No rights

Functional area	Description	Possible permissions
Group of functional areas: Data retrieval and analysis		
Retrieve and analyze data	Managing data retrieval and analysis	• Manage • Read • No rights

Functional area	Description	Possible permissions
Group of functional areas: Tasks		
Retroscan	Managing retroscan background task	• Manage • Manage created • Read • No rights
Exporting events	Managing event export background task	• Manage • Manage created • Read • No rights
KTL	Managing KTL query background task	• Manage • Manage created • Read • No rights
KATA	Managing KATA query background task	• Manage • Manage created • Read • No rights
Download assets	Managing KSC/KICS asset download background task	• Manage • Manage created • Read • No rights
Download user accounts	Managing the download Active Directory user accounts background task	• Manage • Manage created • Read • No rights
Update KUMA content	Managing the update KUMA content background task	• Manage • Manage created • Read • No rights
Clear history	Managing clear resource history background task	• Manage • Manage created • Read • No rights
Update monitoring policy files	Managing the update monitoring policy files background task	• Manage • Manage created • Read • No rights
Export event sources	Managing the export event sources to CSV format background task	• Manage • Manage created • Read • No rights
KIRA	Managing background task, viewing KIRA query results and deobfuscation	• Manage • Manage created • Read • No rights
Searching events in the background	Managing the background event search background task	• Manage • Manage created • Read • No rights
Backing up partitions	Managing partition backup background task	• Manage • No rights

Functional area	Description	Possible permissions
Restoring partitions from backup	Managing the restore partitions from backup background task	• Manage • No rights
Import partition backup	Managing import partitions backup background task	• Manage • No rights
Group of functional areas: Settings		
Subgroup: Access – Users		
Common	Managing users	• Manage • Manage created • Read • No rights
No tenant access	Managing users that do not have access to tenants	• Manage • No rights
Credentials	Managing the creation of a REST API access token, changing a password	• Manage • Manage created • No rights
Subgroup: Access – Roles		
Roles	Managing custom role settings	• Manage • Read • No rights
Common	Managing the assignment of roles to users (except for the General administrator)	• Manage • Read • Read created • No rights
General administrator	Managing the assignment of the General administrator role	• Manage • No rights
CyberTrace administrator	Managing the administrator role in the CyberTrace web console	• Manage • No rights
Subgroup: Access – Tenants		
Tenant registry	Managing the list of tenants	• Manage • Read
Settings	Managing KUMA-specific tenant settings (for example, EPS limits)	• Manage • No rights
Subgroup: Access – Active Directory		
Managing domain authentication settings	Managing ActiveDirectory, FreeIPA authorization settings	• Manage • Read • No rights
Accounts	LDAP server integration by tenant	• Manage • Read • No rights
Account details	Active Directory account details	• Read • No rights
Subgroup: Access – Security policies		
Security policies	Managing security policy configuration	• Manage • Read • No rights
Subgroup: Access – Access to spaces		
Actions with space sets	Managing event space sets	• Manage • No rights
Assigning space sets to users	Assigning and reading custom space sets; assigning default space sets	• Manage • No rights

Functional area	Description	Possible permissions
Subgroup: Integration		
KTL	Managing KTL integration settings	• Manage • Read • No rights
cybertrace	Managing CyberTrace integration settings	• Manage • Read • No rights
KSC	Managing KSC updates	• Manage • Read • No rights
KIRA	Managing KIRA integration settings	• Manage • Read • No rights
KSN	Managing KSN integration settings	• Manage • Read • No rights
KICS	Managing KICS integration settings	• Manage • Read • No rights
KATA single	Managing KATA integration settings	• Manage • Read • No rights
KATA multi	Managing KATA integration settings (distributed solution)	• Manage • Read • No rights
NCIRCC	Managing NCIRCC settings	• Manage • No rights
KSN	Managing KSN integration settings	• Manage • Read • No rights
KASAP	Managing KASAP integration settings	• Manage • Read • No rights
KIRA	Managing KIRA integration settings	• Manage • Read • No rights
KSN	Managing KSN integration settings	• Manage • Read • No rights
Subgroup: Alerts		
Linking segmentation rules to alerts	Managing the linking of segmentation rules to alerts	• Manage • Read • No rights
Linking notification templates to alerts	Managing the linking of notification templates to alerts	• Manage • Read • No rights
Alerts	Managing alert creation settings and alert event storage	• Manage • Read • No rights
Subgroup: License		
License	Managing licensing	• Manage • Read
Subgroup: Incidents		
Incidents	Managing incident configuration	• Manage • Read • No rights

Functional area	Description	Possible permissions
Subgroup: KUMA repository update		
Updating the KUMA repository	Managing KUMA repository update settings	• Manage • Manage created • Read • No rights
Subgroup: Assets		
Importing assets	Managing asset import settings	• Manage • Read • No rights
Asset audit	Managing asset audit settings	• Manage • Read • No rights
KSC	Managing KSC asset import settings	• Manage • Read • No rights
Subgroup: Resource tag list		
Resource tag list	Managing KUMA resource tags	• Read • No rights
Subgroup: Service monitoring		
Service monitoring. Configuring thresholds	Managing thresholds for alerts of each type of service	• Manage • Read • No rights
Subgroup: Extended event schema fields		
Deleting and modifying KUMA extended event schema fields	Deleting and toggling the `disabled` status of KUMA extended event schema fields	• Manage • No rights
KUMA extended event schema fields	Managing KUMA extended event schema fields (except for deleting and toggling the `disabled` status)	• Manage • Read • No rights
Subgroup: Ignore TTL		
Ignore TTL	Managing the ignore TTL setting	• Manage • No rights
Subgroup: Event source discovery		
Event source discovery	Managing event source discovery settings	• Manage • Read • No rights
AI score and AI status of assets		
AI score and AI status of assets	Managing API configuration for `sequence appraiser` setting	• Manage • No rights
Subgroup: Rvision		
Rvision	Managing Rvision settings	• Manage • No rights
Subgroup: Access to REST API permissions settings		
Access to REST API permissions settings	Managing the list of available endpoints settings	• Manage • Manage created • No rights

Functional area	Description	Possible permissions
Group of functional areas: System operations		
Creating a backup copy	Creating a backup copy of KUMA Core	• Manage • No rights
Restoring	Restoring KUMA from a backup copy.	• Manage • No rights
KUMA web application certificates	Managing KUMA web application certificate	• Manage • No rights
KUMA internal certificates	Managing KUMA internal certificates	• Manage • No rights
Maintenance	Maintenance	• Manage • No rights
Group of functional areas: CyberTrace		
cybertrace	CyberTrace Web Console access	• Read • No rights
Group of functional areas: Event sources		
Event sources	Managing event sources	• Manage • Read • No rights
Monitoring policies	Managing monitoring policies	• Manage • Read • No rights
Inline monitoring policies	Managing inline monitoring policies	• Manage • No rights
Group of functional areas: Predefined entities		
Predefined entities	Managing predefined entities	• Manage • Read • No rights
Group of functional areas: Notifications		
Receiving SMTP notifications	Receiving SMTP notifications	• Read • No rights

Editing user role settings

You cannot manage the settings of predefined system roles. You can duplicate a predefined role and view the cards of roles (the permissions of a role and the users to which the role is assigned).

To manage the settings of a custom role:

1. In the **Settings** → **Access** → **Roles** section, click the name of the custom role in the Name column of the table of roles.

2. On the displayed sidebar, enable or disable the toggle switch to activate or deactivate the role, if necessary.

   When you change the state of a role to make it inactive, the role becomes unavailable for assignment to users. If this role has been assigned to a user, the permissions granted by the role are stripped from the user. If this role was the only role assigned to the user, the user's session is terminated. In the **Settings** → **Access** → **Users** section, such a user is no longer displayed among active users, but is instead listed among inactive users. The card of such a user displays a warning about needing to assign at least one role to the user or to delete the user.

When you change the state of a role to make it active, the role is added to the list of roles that can be assigned to a user.

After activating a role, the user to which this role is assigned does not automatically become an active user in the **Settings** → **Access** → **Users** section. You need to activate the user.

By default, a custom role is created in an active state.

3. If necessary, edit the name, description, and permissions of the custom role. You can use the **Show functional areas** filter to select the authorization level that you need. KUMA displays only those functional areas to which your selected permissions have been assigned.

4. Click the **Save** button.

Viewing role settings

To view the set of permissions of a role:

In the **Settings** → **Access** → **Roles** section, click a role name in the **Name** column of the table of user roles.

In the displayed sidebar on the right, under **List of permissions**, a set of permissions by functional area is displayed for the role.

To view the list of users with the selected role and tenants in which the role will be assigned to users:

1. Go to the **Settings** → **Access** → **Roles** section.

2. Do one of the following:

   - Click the number indicated for the role in the **Users** column of the table of roles.

   - Click the name of the role in the **Name** column to open a window, and in that window, select the **Users and groups** tab.

   The opened window displays users to which the role has been assigned. You can view active and inactive users with their names, login names, email addresses. For each user, the number of assigned roles and the tenant of the user are also indicated. Clicking the link with the number specified for the role in the **Users** column lets you edit the user account.

Deleting a user role

To delete custom roles:

1. In the **Settings** → **Access** → **Roles** section, select check boxes to pick the role or roles that you want to delete.

2. Click the **Delete** button above the table of roles.

   The **Delete** button becomes clickable only when you select some custom roles for deletion. Predefined roles cannot be deleted.

3. To confirm deletion, do one of the following:

   - If the role has been assigned to a user, enter the confirmation code and click **OK**.

   - If the role has not been assigned to a user, click **OK**.

   KUMA removes the role from the list of roles, and permissions of the role are stripped from the users that had this role assigned. When a role is deleted while a session is active for users that have no other roles but this one, the sessions of such users are terminated. Assign other roles to such users or delete them.

Configuring the security policy for logging in to the web interface

To reduce the risk of unauthorized access to the KUMA web interface, you can configure rules for users logging in to the KUMA web interface. For example, configuring a security policy helps prevent an attacker from brute-forcing a password to log in to the KUMA web interface.

The security policy applies only to user accounts created in KUMA and does not affect domain accounts imported into KUMA when integrating with domain controllers. At the same time, the security policy affects the admin user account, which is used for the first login to the KUMA web interface, in a limited way. The only security policy setting that applies to this user account is the forced re-authentication requirement after a period of inactivity.

The security policy applies to all tenants and cannot be configured on a per-tenant basis.

When upgrading from a previous version of KUMA, the password requirements apply only to new passwords. Existing passwords are affected only by the **Password lifetime (days)**, other requirements do not apply to such passwords. For users whose passwords have not been changed for more than 90 days, KUMA suggests a password change after the upgrade.

Managing security policy settings requires the General administrator role.

To configure the security policy for logging in to the KUMA web interface

1. Open the **Settings** → **Access** → **Security policy settings** section of the KUMA web interface.

2. Specify the following security settings:

   - **Maximum number of failed authentications**. If this value is exceeded, the user account is locked out for a duration specified in the **Blockage period after failed authentication attempts (mins)** setting. Enter a number from 0 to 10. The default setting is 0, meaning that this setting is disabled.

   - **Maximum number of authentication attempts per second per Core**. This setting helps prevent brute-forcing a password to log in to the KUMA web interface. Enter a number from 1 to 8. The default value is 3. If KUMA detects that the specified value is exceeded, further authentication attempts are blocked.

     Note that the value is specified per KUMA Core. If your KUMA instance has more than one KUMA Core deployed, the actual number of allowed authentication attempts per second is calculated as the specified value multiplied by the number of KUMA Cores.

   - **Blockage period after failed authentication attempts (mins)**. The duration for which the user account is locked out when the value of the **Maximum number of failed authentications** setting is exceeded. Enter a number from 0 to 1440. The default value is 15. If 0, the account status is changed to *Inactive*. A user with this status cannot log in to the KUMA web interface. The General administrator can change the user account status later. If the General administrator changes the status of a user account to *Active*, the user account is unlocked and the counter of failed login attempts is reset to 0.

- **Prevent users from signing in after the password expiration**. This setting allows you to configure the behavior of the solution after the expiration of the **Password lifetime (days)**.

  If this setting is enabled, the user is locked out of the KUMA web interface. The user account status changes to *Inactive*. A user with this status cannot log in to the KUMA web interface. The General administrator can change the user account status later. The user is locked out if the user has the **User must change password at next login** setting enabled.

  If this setting is disabled, the user with an expired password can log in to the KUMA web interface. KUMA then automatically prompts the user to change the password.

- **Re-authentication is required after the user is inactive for (mins)**. If no mouse movement or key presses are registered for the specified time during a user's KUMA web interface session, KUMA requires the user to authenticate again. Enter a number from 1 to 1440. The default value is 15.

3. Specify the following user password settings:

   - **Password lifetime (days)**. After the password lifetime expires, KUMA locks out or does not lock out the user account, depending on the **Prevent users from signing in after the password expiration** setting. Enter a number from 1 to 365. The default value is 90.

   - **Minimum password length (symbols)**. Specify a number from 16 to 128. The default value is 16.

   - **Time to notify the user before the password expiration (days)**. When the specified number of days remains before the password expires, the user is prompted in the KUMA web interface to change the password. Enter a number from 1 to 14. The default value is 14.

   - **Character categories a password must include**. You can use this setting to configure requirements that apply to manually entered and automatically generated passwords:

     - The password must contain lowercase and uppercase letters of the Latin alphabet, numerals, and at least one of the special characters that you specified.

     - **Ignore repeated characters in the password**. If this check box is selected, two or more identical characters in a row are allowed in passwords.

4. Click **Save**.

Security policy is configured.

Creating a user account

To create a user account:

1. In the KUMA web interface, open **Settings** → **Access** → **Users**.

2. Click the **Create new** button and set the parameters as described below.

   - Enabling the **Active** toggle switch makes the user account active. The toggle switch is turned on by default.

     Only users with an *Active* account can log in to the KUMA web interface. The status of a user account can also change to *Inactive* automatically. For example, this might happen if the maximum allowed number of attempts to log in to the solution web interface is exceeded while the **Blockage period after failed authentication attempts** is set to 0.

   - In the **Name** field, enter the user name. The length of the string must be 1 to 128 Unicode characters.

- In the **Login** field, enter a unique user name for the user account. Must contain from 3 to 64 characters (only a–z, A–Z, 0–9, . \ - _).

- In the **Email** field, enter the unique email address of the user. Must be a valid email address.

- In the **Time zone** field, select the time zone in which you want timestamps to be displayed in KUMA. The list is generated based on the settings of the user's operating system and takes into account daylight saving time. The timezone of the user's browser is used by default.

- Select the **Use ISO 8601 format** to display timestamps in ISO 8601 format (for example, 2026-02-08T17:35:27+03:00). This format is used in those sections of the KUMA web interface that use an abbreviated or full display of the date and time, and is applied throughout the KUMA system. The configured format is saved in the KUMA Core settings.

- Select the **Receive email notifications** check box if you want the user to receive SMTP notifications from KUMA.

- Select the **Notify about alerts in web interface** check box to display alert notifications in the KUMA web interface. Clear this check box if you want to disable notification display. This check box is selected by default.

- Select the **Display non-printable characters** check box to display non-printing characters such as spaces, tab characters, and line breaks in the KUMA web interface. If the **Display non-printable characters** check box is selected, you can press **`Ctrl`**/**`Command`**+**`*`** to enable or disable the display of non-printing characters.

  Spaces and tab characters are displayed in all input fields (except the **Description** field), in normalizers, correlation rules, filters and connectors, and in SQL queries for searching events in the **Events** section. Spaces are displayed as dots. A tab character is displayed as a dash in normalizers, correlation rules, filters and connectors. In other fields, a tab character is displayed as one or two dots.

  Line break characters are displayed in all input fields that support multi-line input, such as the event search field.

- In the **New password** field, enter a new password. You can enter a password or generate one by clicking the **Generate password** button. The password must satisfy the following requirements:

  - The length must satisfy the security policy.

  - At least one lowercase character.

  - At least one uppercase character.

  - At lease one numeral.

  - At least one special character from the list of special characters in the security policy.

  - No more than two identical characters in a row.

  - The password does not contain the login.

The user must change the password when logging in to the KUMA web interface for the first time and subsequently change the password at least once every three months. The General administrator can manage both of these settings in the security policy.

- In the **Confirm password** field, enter the password again for confirmation.
- If the **User must change password at next login** check box is selected, the next time the user attempts to log in to the KUMA web interface, the user must specify the old password and set a new password. After that, the user is allowed to log in to the KUMA web interface with the new password. By default, this check box is selected.

  This setting is available only for *Active* accounts.

  You can use this setting, for example, when creating a user. You can assign a temporary password to the user and select this check box. After the user logs in with a temporary password, KUMA prompts the user to change the password.

  You can also make users reset their passwords in the **Settings** → **Access** → **Users** section by selecting users from the list and clicking the **Reset password at next login** button.
- Under **Access**, click the **Add role groups** buttons to assign roles to the user account in specific tenants. A user can be assigned different roles in different tenants; multiple roles can be assigned within the same tenant.
- In the **Space sets** drop-down list, select check boxes next to one or more space sets to which you want to grant access. If the user does not have a space set selected, access is granted to the default space set.
- If the **Unlimited password lifetime** check box is selected, the **Password lifetime** setting does not apply to the user account.

  We recommend enabling this setting for a service account, restricting the rights of such an account, and setting a password of maximum complexity. Typically, a user account with an unlimited password lifetime is used for monitoring. When migrating users, you can manually enable this setting for those service accounts that were previously used to display the dashboard.

3. If necessary, use the **Generate token** button to generate an API token.

   Clicking this button displays the token creation window.
4. If necessary, configure the operations available to the user via the REST API by using the **API access rights** button.
5. Click **Save**.

The user account will be created and displayed in the **Users** table.

Editing a user account

To edit a user account:

1. In the KUMA web interface, open **Settings** → **Access** → **Users**.
2. Select the relevant user and in the user details area on the right, edit the settings as necessary.

If you want to change your own user account, you can also click the name of the user account in the lower left corner of the window to open a menu and click the **Profile** button in the menu.

- Selecting the **Active** check box makes the user account active. The toggle switch is turned on by default.

  A user cannot deactivate their own user account.

  Only users with an *Active* account can log in to the KUMA web interface. The status of a user account can also change to *Inactive* automatically. For example, this might happen if the maximum allowed number of attempts to log in to the solution web interface is exceeded while the **Blockage period after failed authentication attempts** is set to 0.

- In the **Name** field, edit the user name. The length of the string must be 1 to 128 Unicode characters.

- In the **Login** field, enter a unique user name for the user account. Must contain from 3 to 64 characters (only a–z, A–Z, 0–9, . \ - _).

- In the **Email** field, edit the unique email address of the user. The email address must be valid and unique.

- In the **Time zone** field, select the time zone in which you want timestamps to be displayed in KUMA. The list is generated based on the settings of the user's operating system and takes into account daylight saving time. The timezone of the user's browser is used by default.

- Select the **Use ISO 8601 format** to display timestamps in ISO 8601 format (for example, 2026-02-08T17:35:27+03:00). This format is used in those sections of the KUMA web interface that use an abbreviated or full display of the date and time, and is applied throughout the KUMA system. The configured format is saved in the KUMA Core settings.

- Select the **Receive email notifications** check box if you want the user to receive SMTP notifications from KUMA.

- Select the **Notify about alerts in web interface** check box to display alert notifications in the KUMA web interface. Clear this check box if you want to disable notification display. This check box is selected by default.

- Select the **Display non-printable characters** check box to display non-printing characters such as spaces, tab characters, and line breaks in the KUMA web interface. If the **Display non-printable characters** check box is selected, you can press **`Ctrl/Command+*`** to enable and disable the display of non-printing characters.

  Spaces and tab characters are displayed in all input fields (except the **Description** field), in normalizers, correlation rules, filters and connectors, and in SQL queries for searching events in the **Events** section. Spaces are displayed as dots. A tab character is displayed as a dash in normalizers, correlation rules, filters and connectors. In other fields, a tab character is displayed as one or two dots.

  Line break characters are displayed in all input fields that support multi-line input, such as the event search field.

- Under **Access**, use the **Add role groups** buttons to assign roles to the user in specific tenants. A user can be assigned different roles in different tenants; multiple roles can be assigned within the same tenant. For a domain user, the ability to change the main role (General administrator, Tenant administrator, Tier 2 analyst, Tier 1 analyst, Junior analyst) is blocked in the user card, while additional roles can be added or removed (Access to CII, Interaction with NCIRCC, Read shared resources), including management of additional role assignment to tenants.

- In the **Space sets** drop-down list, select check boxes next to one or more space sets to which you want to grant access. If the user does not have a space set selected, access is granted to the default space set.

3. If you need to change the password, click the **Change password** button and fill in the fields described below in the opened window. When finished, click **OK**.

   - In the **Old password** field, enter the current password of the user account. The field is available if you change your account password.

   - In the **New password** field, enter a new password. You can enter a password or generate one by clicking the **Generate password** button. The password must satisfy the following requirements:

     - The length must satisfy the security policy.

     - At least one lowercase character.

     - At least one uppercase character.

     - At lease one numeral.

     - At least one special character from the list of special characters in the security policy.

     - No more than two identical characters in a row.

     - The password is different from the last three passwords of this account.

     - The password does not contain the login.

   - In the **Confirm password** field, enter the password again for confirmation.

   - If the **User must change password at next login** check box is selected, the next time the user attempts to log in to the KUMA web interface, the user must specify the old password and set a new password. After that, the user is allowed to log in to the KUMA web interface with the new password. This check box is selected by default.

     This setting is available only for *Active* accounts.

4. If necessary, use the **Generate token** button to generate an API token. Clicking this button displays the token creation window.

5. If necessary, configure the operations available to the user via the REST API by using the **API access rights** button.

6. If the **Unlimited password lifetime** check box is selected, the **Password lifetime** setting does not apply to the user account.

   We recommend enabling this setting for a service account, restricting the rights of such an account, and setting a password of maximum complexity. Typically, a user account with an unlimited password lifetime is used for monitoring. When migrating users, you can manually enable this setting for those service accounts that were previously used to display the dashboard.

7. Click **Save**.

The user account will be changed.

Changing the account password

This article describes how to change your or another user's account password.

Changing your account password

To change your account password:

1. Open the KUMA web interface in a browser:

   ```
   https://<IP address or FQDN of a KUMA Core server>:7220
   ```

2. Enter your user name and password.

   If you are logging in for the first time, use the default credentials:

   - Login:

     ```
     admin
     ```

   - Password:

     ```
     mustB3Ch@ng3d!
     ```

3. After logging in, click the user name in the lower left corner of the web interface and select **Profile** from the menu that opens.

4. On the **User** pane on the right, in the **Password** section, click **Change password**.

5. In the **Change password** window, perform the following actions:

   a. Enter the current password in the **Old password** field.

   b. Enter a new password in the **New password** field.

      You can click the **Generate password** button. A new password will be generated according to the password requirements, and the **New password** and **Confirm password** fields will be filled in automatically. If necessary, copy the generated password and store it in a secure location, for example, in the corporate password manager.

   c. In the **Confirm password** field, re-enter the new password.

6. Click **Save**.

The password is changed.

Changing a user account password

Only a user with the General Administrator role can change a user account password.

To change a user account password:

1. In the KUMA web interface, go to the **Settings** → **Access** → **Users** section.

2. In the accounts table, click the user account whose password you want to change.

3. In the **User** window that opens, in the **Password** section, click **Change password**.

4. In the **Change password** window, perform the following actions:

   a. Enter a new password in the **New password** field.

      You can click the **Generate password** button. A new password will be generated according to the password requirements, and the **New password** and **Confirm password** fields will be filled in automatically. If necessary, copy the generated password and store it in a secure location, for example, in the corporate password manager.

   b. In the **Confirm password** field, re-enter the new password.

5. Send new password to the user in a secure way, for example, by encrypted email.

6. If you want the user to use the generated password and set their own new password at the next login to the KUMA web interface, select the **User must change password at next login** check box.

   By default, this check box is enabled. This setting is only available for accounts with the *Active* status. The status of the account can be changed.

7. If necessary, select or clear the **Do not limit password lifetime** check box.

   When the check box is selected, the account password is not affected by the **Password lifetime (days)** setting.

8. Save your changes.

The account password is changed. The user can log in to the KUMA web interface using the new password.

Special considerations involved in changing the set of spaces assigned to a user

A user is assigned one or more space sets; information about these is stored in the user account settings. To view spaces in a space set, hover over the space set in the user profile. If necessary, you can add or remove spaces from the space set in the **Settings** → **Access** → **Access to spaces** section.

If a space is deleted from the storage, the space is still displayed as part of the space set with the `deleted+UUID` designation. In this case, only the first 8 characters of the space's universal unique ID (UUID) are displayed. A deleted space is longer displayed as part of the space set after you save changes to that space set.

> A space is completely deleted from the space set if that space has no events. If there are some events in the space being deleted, KUMA displays the space as `deleted+UUID` even after saving changes to the space set.

Configuring notifications

In KUMA, you can configure the following types of notifications:

- Notifications about alerts in the web interface.

  To display alert notifications in the web interface, select the **Notify about alerts in web interface** check box in user profile.

- Email notifications.

  You can enable sending of standard notifications about the following events:

  - A report is created.
  - An alert is created.
  - An alert is assigned to a user.
  - Task is completed.
  - New resource packages are available and can be obtained by updating the KUMA repository.
  - The daily average EPS has exceeded the limit set by the license.
  - The hourly average EPS has exceeded the limit set by the SMB license.

You can also configure custom notification templates for events about creating an alert, generating a report, completing an asynchronous task, violating a monitoring policy, or moving a user to another KASAP group.

To send notifications by email, you need to connect an SMTP server and select the **Receive email notifications** check box in the user profile.

- Telegram notifications about triggering of the KUMA correlation rules.

Connecting to an SMTP server

To send email notifications, the solution must be connected to SMTP server.

Only one SMTP server can be added.

To connect an SMTP server:

1. In the KUMA web interface, open the **Settings** → **Other** → **General** section.
2. Under **SMTP server settings**, perform the following steps:
   a. Use the **State** toggle switch to enable connection to an SMTP server.
   b. In the **Host** field, specify the address of the SMTP host in one of the following formats: hostname, IPv4, IPv6.
   c. In the **Port** field, specify the port for connecting to the mail server. The value must be an integer from 1 to 65,535.
   d. In the **Secret** drop-down list, select or create a secret of the **credentials** type that contains account credentials for connecting to the SMTP server.

      How to create a secret

      To create a secret:

      1. In the **Name** field, enter the name of the secret.
      2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector.
      3. If necessary, enter a description of the secret in the **Description** field.
      4. Then click the **Create** button.

      The secret is added and displayed in the **Secret** drop-down list.

   e. If necessary, in the **Alias for KUMA Core server** field, enter the name of a KUMA Core server that is used in your network. This name must be different from the FQDN.
   f. In the **From** field, enter an email address of the sender. For example, `kuma@company.com`.
   g. If you don't want to receive notifications about the status of event sources, enable the **Disable monitoring notifications** toggle switch.

      If notifications are enabled in KUMA and there are event sources with a red status, and no notifications have been sent yet, you will receive a single notification for the entire period—even if the status of the sources has changed several times when the sending of notifications was turned off.

h. If notifications about the state of event sources are enabled, select the notification sending frequency from the **Monitoring notifications interval** drop-down list.

   Notifications on a monitoring policy triggering are sent by the source repeatedly within the selected period until the source's status turns green.

   If you select **Notify once**, the notification about the monitoring policy triggering is sent only once during the whole time when the source has the red status. However, a notification on the monitoring policy triggering is sent every time the source status changes from red to green.

i. Click the **Test connection** button. KUMA will send a test message to the email address specified in the current user profile. The test message will be sent even if the **Receive email notifications** check box is not selected in the user profile.

   Check your email inbox. If the test message is delivered, the SMTP server is configured correctly. If an error occurs while sending the message, check the SMTP server settings. The error is displayed in the interface and also recorded in the KUMA Core log. If the message is sent but not delivered to the mailbox, check the SMTP server log for error messages.

   We recommend sending a test message each time you change the SMTP server settings or notification template.

3. Click **Save**.

The SMTP server connection is now configured, and users can receive email messages from Kaspersky SIEM.

Standard email notifications

To configure Kaspersky SIEM to send email notifications:

1. Configure connection to an SMTP server.

2. Select the **Receive email notifications** check box in the user profile.

When email notifications are enabled, Kaspersky SIEM automatically sends standard notifications for the following events:

- A report is created.

  Users listed in the report template schedule settings receive a notification.

- An alert is created.

  All users receive the notification.

- An alert is assigned to a user.

  Notification is sent to a user, to whom the alert was assigned.

- Task is completed.

  Notification is sent to the users who created the task.

- New resource packages are available and can be obtained by updating the Kaspersky SIEM repository.

  The notification is sent to users whose email addresses are specified in the task settings.

- Monitoring policy is triggered.

  When a monitoring policy is triggered, Kaspersky SIEM creates an alert and may send a notification to the email addresses specified in the monitoring policy settings. For configuring notifications based on a monitoring policy, see the Creating a monitoring policy section.

- The daily average EPS has exceeded the limit set by the license.

  A notification is sent to the email addresses of users with the General Administrator user role.

- The hourly average EPS has exceeded the limit set by the SMB license.

  A notification is sent to the email addresses of users with the General Administrator user role.

Notifications about problems with active services

Kaspersky SIEM periodically checks the state of active services and sends out email notifications if any problems are detected. Such notifications are sent to users with the General Administrator role that have the **Receive email notifications** check box selected in their profile.

Notifications about problems with services are sent once every 6 hours. The six hours are counted down from the moment when the **Receive email notifications** check box is selected. If the KUMA Core is restarted, the interval countdown starts over.

If the Warning field is populated for one or several active services during the check, Kaspersky SIEM sends only one summary message. This message contains information about all active services for which any problems were detected. If there are no active services with a filled-in Warning field, no notification is sent.

Custom notification templates

Notification templates are used to create email notifications about events of the following types:

- **Alert created**.

  When you create a notification template for this type of event, you must also create a notification rule that specifies correlation rules and email addresses. When an alert is created based on the selected correlation rules, notifications created based on these templates will be sent to the specified email addresses. Standard KUMA notifications about the same event will not be sent to the specified addresses.

- **Report generated**.

- **Task finished**.

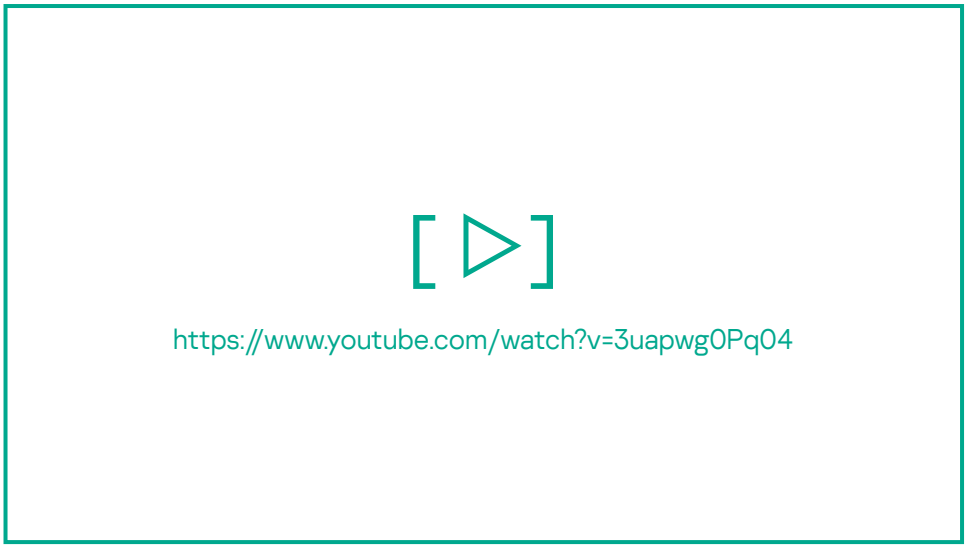
- **Sources monitoring alert**.

- **KASAP group changed**.

For the Shared tenant, you can create event templates of all types. For all other tenants, only the following event types are available: **Alert created** and **Sources monitoring alert**.

By default, the Kaspersky SIEM distribution kit includes a notification template: **[OOTB] New alert in KUMA**. This template can be removed, but it is not available for editing.

To learn more about customizing notification templates, watch this video:



Managing notification templates

This article describes how to create, edit, and delete notification templates.

Creating a notification template

To create a notification template:

1. In the web interface, open **Resources** → **Notification templates**.

   A table of notification templates is displayed.

2. In the toolbar, click the **New** button and configure the settings in the window that opens:

   a. In the **Name** field, enter a name for the notification template. The name must be unique and contain 1 to 128 Unicode characters. The name may not begin or end with a space, and may not contain control sequences (e.g., line feed).

   b. In the **Tenant** drop-down list, select the tenant that will own the notification template.

   > For the Shared tenant, you can create templates for all types of events. For all other tenants, only the **Alert created** and **Sources monitoring alert** types are available.

   c. In the **Type** drop-down list, select the type of event for which you create the notification template:

   - **Alert created**.

     When creating a notification template for this type of event, you also need to create a notification rule.

   - **Report generated**.

- **Task finished**.

  You can create only one template for events of this type. If such a template already exists, this type will not be available for selection when creating a new template.

- **Sources monitoring alert**.

- **KASAP group changed**.

d. In the **Subject** field, enter the subject of the message. Maximum field length: 140 Unicode characters. You can enter the text in English or Russian, depending on the localization selected in the user profile.

   For each event type, a standard subject text is available when creating a template. You cannot edit the text in the **Subject** field or select a standard text until you select the template type in the **Type** field.

   In the subject of the message, you can reference the object fields depending on the selected type of event.

   Example (subject in notification template for an event of the **Alert created** type):

```
New alert in KUMA: {{.CorrelationRuleName}}
```

   In place of `{{.CorrelationRuleName}}`, the subject of the notification message will include the name of the correlation rule contained in the `CorrelationRuleName` alert field.

e. In the **Template** field, enter the text of the message. You can enter the text in English or Russian, depending on the localization selected in the user profile.

   The template syntax allows you to dynamically populate a notification with data from the specified fields of the corresponding objects. For each event type, a standard email message subject text is available when creating a template.

   For convenience, you can open the text of the email message in a separate window by clicking the ⤢ icon. In the **Template** window that opens, you can change the text of the message with notification. Click **OK** to save the changes and close the window.

f. If necessary, add tags for the generated notification template.

   The list includes all available tags created in the tenant of the resource and in the Shared tenant. You can find a tag in the list by typing its name in the field. If the tag you entered does not exist, you can create it by pressing **`Enter`** or clicking **Add**.

g. If necessary, add a description of the template. Maximum length: 4000 Unicode characters.

3. Click **Save**.

The notification template is created and displayed in the **Notification templates** table.

Editing a notification template

To edit a notification template:

1. In the web interface, open **Resources** → **Notification templates**.

   A table of notification templates is displayed.

2. Click the template that you want to change, and in the window that opens, change the necessary settings (see the instructions for creating a notification template).

3. Click **Save**.

The notification template is modified.

Deleting a notification template

To delete a notification template:

1. In the web interface, open **Resources** → **Notification templates**.

   A table of notification templates is displayed.

2. Select the check boxes next to the notification templates that you want to delete.

   You can also delete all created notification templates or all notification templates that are displayed on the page. To do this, click the check box next to the Name column and select **Select all** or **Select all on the page** from the drop-down list.

   > You must select at least one check box.

3. Click the **Delete** button.

   A confirmation window opens. If some of the templates being deleted are linked to other resources or services, these are listed in the confirmation window with a note saying that these templates will not be deleted.

4. Click the **Delete** button to confirm deletion.

The selected templates will be deleted.

Notification template syntax

The notification templates use the Go templates syntax. You can use this syntax to dynamically fill notifications with content: load data from the fields of the corresponding objects, insert links, or convert dates to a different format. You can use the template syntax in the subject as well as the body of the message. This article briefly describes the syntax and lists the fields that can be used for certain types of events, and additional functions that can be applied to these fields. You can read more about the syntax in the official Go language documentation.

In the template, you can reference the object fields depending on the selected type of event. The fields of the corresponding objects can contain simple values such as a string or a number:

```
{{ .CorrelationRuleName }}
```

The message will display the alert name, which is the contents of the `CorrelationRuleName` field of the alert data model.

Some fields contain data arrays. For example, alert fields contain related events, assets, and accounts. Such nested objects can be queried by using the `range` function, which sequentially queries the fields of the first 50 nested objects:

```
{{ range .Assets }}
Device: {{ .DisplayName }}, creation date: {{ .CreatedAt }}
{{ end }}
```

When using the `range` function to query a field that does not contain a data array, an error is returned.

The message will display the values of the `DeviceHostName` and `CreatedAt` fields from 50 assets related to the alert:

```
Device: <DisplayName field value from asset 1>, creation date: <CreatedAt field value from asset 1>
Device: <DisplayName field value from asset 2>, creation date: <CreatedAt field value from asset 2>
...
// 50 strings total
```

You can use the `limit` function to limit the number of objects returned by the `range` function:

```
{{ range (limit .Assets 5) }}
<strong>Device</strong>: {{ .DisplayName }},
<strong>Creation date</strong>: {{ .CreatedAt }}
{{ end }}
```

The message will display the values of the `DisplayName` and `CreatedAt` fields from 5 assets related to the alert, with the words "Devices" and "Creation date" marked with the `<strong>` HTML tag:

```
<strong>Device</strong>: <DeviceHostName field value from asset 1>,
<strong>Creation date</strong>: <value of the CreatedAt field from asset 1>
<strong>Device</strong>: <DeviceHostName field value from asset N>,
<strong>Creation date</strong>: <CreatedAt field value from asset N>
...
// 10 strings total
```

Nested objects can have their own nested objects. They can be queried by using nested `range` functions:

```
{{ range (limit .Events 5) }}
    {{ range (limit .Event.BaseEvents 10) }}
    Service ID: {{ .ServiceID }}
    {{ end }}
{{ end }}
```

The message will show ten service IDs (`ServiceID` field) from the base events related to five correlation events of the alert (50 lines in total). Please note that events are queried through the nested `EventWrapper` structure, which is located in the `Events` field in the alert. Events are available in the `Event` field of this structure, which is reflected in the example above. Therefore, if field `A` contains nested structure `[B]` and structure `[B]` contains field `C`, which is a string or a number, to query field `C`, you must specify the path `{{ A.C }}`.

Some object fields contain nested dictionaries in key-value format (for example, the `Extra` event field). They can be queried by using the `range` function with the variables passed to it: `range $placeholder1, $placeholder2 := .FieldName`. The values of variables can then be called by specifying their names. For instance:

```
{{ range (limit .Events 3) }}
    {{ range (limit .Event.BaseEvents 5) }}
```

```
    List of fields in the Extra event field: {{ range $name, $value := .Extra }} {{ $name }} - {{ $value }} <br>
{{ end }}
    {{ end }}
{{ end }}
```

The message will use an HTML tag
 to show key-value pairs from the `Extra` fields of the base events belonging to the correlation events. Data is called from five base events out of each of the three correlation events.

You can use HTML tags in notification templates to create more complex structures. Example table for correlation event fields:

```
<style type="text/css">
  TD, TH {
    padding: 3px;
    border: 1px solid black;
  }
</style>
<table>
  <thead>
    <tr>
        <th>Service name</th>
        <th>Name of the correlation rule</th>
        <th>Device version</th>
    </tr>
  </thead>
  <tbody>
    {{ range .Events }}
    <tr>
        <td>{{ .Event.ServiceName }}</td>
        <td>{{ .Event.CorrelationRuleName }}</td>
        <td>{{ .Event.DeviceVersion }}</td>
    </tr>
    {{ end }}
  </tbody>
</table>
```

Use the **link_alert** function to insert an HTML alert link into the notification email:

```
{{link_alert}}
```

A link to the alert window will be displayed in the message.

Templates also support more complex constructs such as local variable declaration, comparison operators, and control structures. Below is an example of how you can extract the data on max asset category from the alert data and place it in the notifications:

```
{{ $criticalCategoryName := "" }}
{{ $maxCategoryWeight := 0 }}
{{ range .Assets }}
    {{ range .CategoryModels }}
        {{ if gt .Weight $maxCategoryWeight }}
            {{ $maxCategoryWeight = .Weight }}
            {{ $criticalCategoryName = .Name }}
        {{ end }}
    {{ end }}
{{ end }}
{{ if gt $maxCategoryWeight 1 }}
Max asset category: {{ $criticalCategoryName }}
{{ end }}
```

Object fields supported in templates

The following table lists the fields that can be accessed from templates, depending on the type of event.

Supported object fields

Type	Available fields
Alert created	All fields of the alert data model are supported, including nested arrays and structs.
Report generated	`{{ .Tenants }}`—tenants for which the report is created. `{{ .Name }}`—report name. `{{ .StartTime }}`—the beginning of the period for which the report is created, in the "2006-01-02 15:04:05 MSK" format. `{{ .FinishTime }}`—the end of the period for which the report is created, in the "2006-01-02 15:04:05 MSK" format. `{{ .PreviewLink }}`—link for viewing the report. `{{ .DownloadLink }}`—link for downloading the report. Example of adding links to a report notification template: You can `<a href="{{ .PreviewLink }}" target="_blank">` view `</a>` or `<a href="{{ .DownloadLink }}" target="_blank">download</a>` the report.
Task finished	`{{ .Tenants }}`—the tenant in which the task is started. `{{ .TaskKind }}`—the name of the task. `{{ .TaskCreator }}`—the name (login) of the user that created the task. `{{ .StartTime }}`—the start time of the task in the "2006-01-02 15:04:05 MSK" format. `{{ .FinishTime }}`—the end time of the task in the "2006-01-02 15:04:05 MSK" format. `{{ .TaskStatus }}`—task execution status.
Sources monitoring alert	`{{ .SourceTenantName }}`—tenant of the event source. `{{ .SourceDisplayName }}`—name of the source. `{{ .Value }}`—the value that exceeded the bounds of the monitoring policy at the time of the alert creation. `{{ .WebLink }}`—link to the KUMA web interface. `{{ .AlertActiveAt }}`—time at which the alert was active. `{{ .PolicyName }}`—name of the monitoring policy. `{{ .PolicyTenantName }}`—tenant of the monitoring policy. `{{ .PolicyLowerEventBound }}`—lower threshold. `{{ .PolicyUpperEventBound }}`—upper threshold. `{{ .PolicyKind }}`—type of the policy. `{{ .PolicyInterval }}`—interval of the counting period. `{{ .DeviceProduct }}`—source device. `{{ .DeviceHostName }}`—source host name. `{{ .DeviceAddress }}`—MAC address of the source. `{{ .DeviceProcessName }}`—name of the source process.
KASAP group changed	`{{ .UserEmail }}`—display name of the user from Active Directory. `{{ .PreviousGroup}}`—KASAP learning group to which the user belonged at the time when the user's card was opened form an incident or alert. `{{ .CurrentGroup}}`—KASAP training group to which the user was moved from the user's card. `{{ .WebLink }}`—link to the KUMA web interface.

Functions in notification templates

Functions available in templates are listed in the table below.

Function	Description
`date`	Takes the time in milliseconds (unix time) as the first parameter; the second parameter can be used to pass the time in RFC standard format. The time zone cannot be changed. Example call: `{{ date .FirstSeen "02 Jan 06 15:04" }}` Call result: 18 Nov 2022 13:46 Examples of date formats supported by the function: • `"02 Jan 06 15:04 MST"` • `"02 Jan 06 15:04 -0700"` • `"Monday, 02-Jan-06 15:04:05 MST"` • `"Mon, 02 Jan 2006 15:04:05 MST"` • `"Mon, 02 Jan 2006 15:04:05 -0700"` • `"2006-01-02T15:04:05Z07:00"`
`range`	Lets you iterate over arrays or sets of key-value pairs, sequentially referring to the fields of the first 50 items.

`limit`	This function is called inside the `range` function to limit the list of data. It processes lists that do not have keys, takes any list of data as the first parameter and truncates it based on the second value. For example, the `.Events`, `.Assets`, `.Accounts`, and `.Actions` alert fields can be passed to the function.
	Example call:
	`{{ range (limit .Assets 5) }}`
	`<strong>Device</strong>: {{ .DisplayName }},`
	`<strong>Creation date</strong>: {{ .CreatedAt }}`
	`{{ end }}`

`link_alert`	Generates a link to the alert with the URL specified in the SMTP server connection settings as the KUMA Core server alias or with the real URL of the KUMA Core service if no alias is defined. Example call: `You can find more information about the alert in the KUMA web interface: {{link_alert}}.`

`link_task`	Generates a link to the task in KUMA.
	Example call:
	`Task "{{ .TaskKind }}" created {{ .TaskCreator }} at {{ .StartTime }} and completed at {{ .FinishTime }} with the "{{ .TaskStatus }}" status.`
	`You can find more information about tasks in the KUMA web interface: {{ link_task }}.`

`link`	Takes the form of a link that can be followed. Example call: `{{ link "https://support.kaspersky.com/KUMA/2.1/en-US/233508.htm" }}`

Telegram notifications

This integration is an example and may require additional configuration depending on the versions used and the specifics of the infrastructure.
Compatibility is confirmed only for KUMA 2.0 and later.
The terms and conditions of premium technical support do not apply to this integration; support requests are processed without a guaranteed response time.

You can configure sending notifications to Telegram when KUMA correlation rules are triggered.

For example, in Telegram, notifications may be received when the number of incoming events drops below a specified threshold. To do this, create a correlation rule that generates an alert, as well as an alert response rule that will run a script that sends a notification to Telegram.

Configure Telegram notifications involves the following steps:

1 Creating and configuring a Telegram bot

A special bot sends notifications about triggered correlation rules. It can send notifications to a private or group Telegram chat.

To create and configure a Telegram bot:

1. In the Telegram application, find the BotFather bot and open a chat with it.

2. In the chat, click **Start**.

3. Create a new bot using the following command:

   ```
   /newbot
   ```

4. Enter the name of the bot.

5. Enter the login name of the bot.

   The bot is created. You will receive a link to the chat that looks like `t.me/<bot login>` and a token for contacting the bot.

6. If you want to use the bot in a group chat rather than in private messages, then you need to edit privacy settings:

   a. In the BotFather chat, enter the command:

   ```
   /mybots
   ```

   b. Select the relevant bot from the list.

   c. Click **Bot Settings** → **Group Privacy**, and select **Turn off**.

   The bot can now send messages to group chats.

7. To open a chat with the bot you created, use the `t.me/<bot login>` link that you obtained at step 5, and click **Start**.

8. If you want the bot to send private messages to the user, follow the steps below:

   a. In the chat with the bot, send any message.

   b. Follow the `https://t.me/getmyid_bot` link and click **Start**.

   The response contains the `Current chat ID`. You need this value to configure the sending of messages.

9. If you want the bot to send messages to the group chat:

   a. Add `https://t.me/getmyid_bot` to the group chat used for receiving notifications from Kaspersky SIEM.

      The bot sends a message to the group chat, the message contains the `Current chat ID` value. You need this value to configure the sending of messages.

   b. Remove the bot from the group.

10. Send a test message through the bot. To do so, paste the following link into the address bar of your browser:

```
https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test
```

where `<token>` is the value obtained at step 5, and `<chat_id>` is the value obtained at step 8 or 9.

A test message is displayed in a private or group chat. The browser response should contain no JSON errors.

2 Creating a script for sending notifications

You must create a script and save it on the server where the correlator is installed.

To create a script:

1. In the console of the server on which the correlator is installed, create a script file and add the following lines to it:

```
#!/bin/bash
set -eu
CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
RULE=$1
TEXT="<b>$RULE</b> rule triggered"
curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML"
https://api.telegram.org/bot$TG_TOKEN/sendMessage
If the correlator server does not have internet access, you can use a proxy server:
#!/bin/bash
set -eu
CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
RULE=$1
TEXT="<b>$RULE</b> rule triggered."
PROXY=<address and port of the proxy server>
curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode
"parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

2. Save the script to the correlator directory at `/opt/kaspersky/kuma/correlator/<ID of the correlator that will respond to events>/scripts/`.

   For information about obtaining the correlator ID, see the "Getting service identifier" section.

3. Make the "kuma" user the owner of the file and grant them execution rights using the following commands:

```
chown kuma:kuma /opt/kaspersky/kuma/correlator/<ID of the correlator that must respond>/scripts/<script
name>.sh
```

```
chmod +x /opt/kaspersky/kuma/correlator/<ID of the correlator that must respond>/scripts/<script name>.sh
```

3 Configuring notifications in Kaspersky SIEM

Configure a KUMA response rule that starts a script to send notifications and add this rule to the correlator.

To configure sending of Kaspersky SIEM notifications to Telegram:

1. Create a response rule:

   a. In the web interface, open the **Resources** → **Response rules** section and click the **Create** button.

   b. This opens the **Create response rule** window; in that window, in the **Name** field, enter a name for the rule.

   c. In the **Tenant** drop-down list, select the tenant that owns the resource.

   d. In the **Type** drop-down list, select **Run script**.

   e. In the **Script name** field, enter the name of the script.

   f. In the **Script arguments** field, specify:

   ```
   {{.Name}}
   ```

   This passes the name of the correlation event as the argument of the script.

   g. Click **Create**.

2. Add the response rule to the correlator:

   a. In the **Resources** → **Correlators** section, select the correlator in whose folder you placed the created script for sending notifications.

   b. In the steps tree, select **Response**.

   c. Click **Add response rule**.

   d. In the **Response rule** drop-down list, select the rule added at step 1 of these instructions.

   e. In the steps tree, select **Setup validation**.

   f. Click the **Save and restart services** button.

   g. Click the **Save** button.

Sending notifications about triggered KUMA rules to Telegram is configured.

Managing certificates

This section describes how to work with certificates.

Downloading certificates

The following certificates are available for download in the KUMA web interface:

- REST API CA certificate.

  This certificate is used to authenticate the API server serving the KUMA public API. You can also use this certificate when importing data from MaxPatrol reports.

  You can change the certificate if you want to use your company certificate and key instead of the self-signed web interface certificate.

  Once downloaded, the certificate can be imported into the trust storage of the operating system or browser. After that, the client will trust the TLS certificate that was issued by KUMA and signed by the certification authority.

  The downloaded CA certificate is not intended for editing. If you need to change the list of node names (SAN) or use a certificate from a corporate certification authority, you should issue a new TLS certificate and upload it to KUMA in the **Settings** → **Other** → **Common** → **External TLS pair**.

  For an installation in a high availability configuration in a Raft cluster without a balancer, you can download the CA certificate of the REST API to any node, but a secure connection is available for the core-1 node only. The rest of the nodes return an error. If you want to directly log in with the same certificate to all nodes of the Raft cluster without a balancer, when generating a certificate, you can specify the FQDNs of all KUMA Core nodes in the Raft cluster in the `Subject Alternative Names` (SAN) field.

  The FQDN of nodes in the Subject Alternative Names (SAN) field is specified at the stage of issuing a new TLS certificate. You do not need to modify the downloaded REST API CA certificate.

  If the cluster contains multiple nodes running the KUMA Core service and direct connections to each node are expected, it is recommended to use a TLS certificate whose SAN includes the FQDNs of all KUMA Core nodes. Otherwise, the browser may display a warning that the node name does not match the certificate.

- Microservice CA certificate.

  This certificate is used for authentication when connecting log sources to passive collectors using TLS, but without specifying your own certificate.

- AI service certificate.

  This certificate is required to install the **AI-rating and AI-status of assets** service.

To download a certificate:

1. In the KUMA web interface, go to the **Resources** → **Active services** section.
2. Select the check box next to the KUMA Core service.
3. In the toolbar, in the (⋮) menu select a command:
   - **Download REST API CA certificate**
   - **Download Microservice CA certificate**
   - **Download AI service certificate**

The certificate is saved to the folder specified in your browser settings.

To copy the certificate fingerprint:

1. In the KUMA web interface, go to the **Resources and services** → **Active services** section.

2. In the toolbar, from the menu (⋮), select **Copy fingerprint**.

   The fingerprint certificate ID is copied to the clipboard. Use the fingerprint ID of the CA certificate as the value of the `--pair.fingerprint` option in the service installation command for validation of the KUMA Core certificate when the service connects to the KUMA Core for the first time.

Modifying the self-signed web interface certificate

You can use your company certificate and key instead of a self-signed web interface certificate. For example, if you want to replace a self-signed CA Core certificate with a certificate issued by an enterprise CA, you must provide an `external.cert` and an unencrypted `external.key` in PEM format.

The provided instruction shows how to replace a self-signed CA Core certificate with an enterprise certificate in PFX format. You can use the instructions as an example and adapt the steps according to your needs.

To replace the KUMA web interface certificate with a corporate certificate in PFX format:

1. If you are using a certificate and key in a PFX container, use OpenSSL to convert the PFX file to a certificate and an encrypted key in PEM format:

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nokeys -out external.cert
   ```

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nocerts -nodes -out external.key
   ```

   When carrying out the command, you are required to specify the PFX key password (Enter Import Password).

   You will receive the `external.cert` certificate and the `external.key` in PEM format.

2. If your `external.key` is not encrypted, make sure that the key is in PKCS#8 format. Kaspersky SIEM will not be able to process a key file if it starts with the `BEGIN RSA PRIVATE KEY` tag. In this case, convert the file using the command:

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   Once the command is executed, the file will start with the `BEGIN PRIVATE KEY` tag, and Kaspersky SIEM will process the key file.

3. In the web interface, open the **Settings** → **Other** → **General** section.

4. Under **External TLS pair**, upload the `external.cert` and the unencrypted `external.key` in PEM format.

5. Restart Kaspersky SIEM:

```
systemctl restart kuma-core
```

6. Refresh the web page or restart the browser that you use to manage the web interface.

Your company certificate and key have been replaced.

Reissuing internal CA certificates

Only users with the General administrator role may reissue internal CA certificates.

To reissue and apply internal CA certificates:

1. In the web interface, open the **Settings** → **Other** → **General** section.

2. Click the **Reissue internal CA certificates** button.

3. Confirm the re-issue of certificates in the window that opens.

   CA certificates for KUMA services and CA certificates for ClickHouse are reissued. Reissued certificates must be applied.

4. Connect to the hosts where the collector, correlator, and event router services are deployed:

   a. Stop all services by running the following command:

   ```
   sudo systemctl stop kuma-<collector/correlator/eventRouter/metrics>-<service_ID>.service
   ```

   where:

   <service_ID> is the service ID copied from the KUMA web interface.

   b. Delete the `internal.cert` and `internal.key` files from the `/opt/kaspersky/kuma/<service type>/<service ID>/certificates` directories using the following commands:

   ```
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.cert
   ```

   ```
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.key
   ```

5. Connect to the hosts where storage services are deployed:

   a. Stop all storage services:

   ```
   sudo systemctl stop kuma-<storage>-<service_ID>.service
   ```

b. Delete the `internal.cert` and `internal.key` files from the `/opt/kaspersky/kuma/storage/<service ID>/certificates` directories by running the following commands:

```
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.cert
```

```
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.key
```

6. Delete all ClickHouse certificates from the `/opt/kaspersky/kuma/clickhouse/certificates` directory using the following commands:

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
```

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
```

7. Connect to the hosts where agent services are deployed:

   a. Stop the services of Windows agents and Linux agents.

   b. Delete the `internal.cert` and `internal.key` files from working directories of the agents.

8. Restart the KUMA Core to apply the new CA certificates:

   - To deploy on a single server and distributed deployment, run the following command:

     ```
     sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
     ```

   - To deploy in a Kubernetes cluster, run the following commands on any controller:

     ```
     sudo k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
     ```

     ```
     sudo k0s kubectl rollout restart deployment metrics -n kuma
     ```

     ```
     sudo k0s kubectl rollout restart deployment/core-deployment -n kuma
     ```

     It is recommended to restart KUMA Core using the command, since restarting through the web interface affects only the restart of the KUMA Core bucket, and not KUMA Core entirely.

9. Go to the **Resources and services** → **Active services** section, select the check box next to the Core service, and in the menu (⋮), select **Copy fingerprint**.

   The fingerprint of the Core's CA certificate is copied to the clipboard.

10. On each host where KUMA services are installed, paste the copied fingerprint as the value of the `--pair.fingerprint` setting in the service's systemd file.

11. Run the following command to apply the changes to the systemd file:

```
sudo systemctl daemon-reload
```

12. Restart all stopped services:

```
sudo systemctl start kuma-<collector/correlator/eventRouter/storage/metrics>-<service_ID>.service
```

where:

<service_ID> is the service ID copied from the KUMA web interface.

The new internal CA certificates are applied.

Reissuing a certificate for a specific service

To reset a certificate for a specific service:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check box next to the service whose certificate you want to reissue.
3. In the toolbar or menu ⋮, select **Reset certificate**.

   This option cannot be used to renew the KUMA Core certificate. To update KUMA Core certificates, they must be reissued and internal CA certificates must be applied.

4. Delete the old certificate in the service installation directory.

   The solution will generate a new certificate automatically. You do not need to restart running services, the new certificate is applied automatically. A stopped service must be restarted to have the certificate applied.

Special considerations for deleting Windows agent certificates:

- If the agent is in green status, KUMA deletes the current certificate and generates a new one. The agent will continue operating with the new certificate.
- If the agent is in a red status, an error is displayed indicating that the agent is not running. In the `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent ID>\certificates` agent installation folder, delete `internal.cert` and `internal.key` files and start the agent manually. When the agent starts, a new certificate is created automatically.

Special considerations for deleting Linux agent certificates:

- The certificate is reset via the web interface regardless of the agent status.
- In the `/opt/kaspersky/agent/<agent ID>/certificates` agent installation folder, delete `internal.cert` and `internal.key` files.
- Since resetting the certificate stops the agent, you must manually start the agent to resume its operation. When the agent starts, a new certificate is created automatically.

Reissuing the AI service certificate

To reissue the AI service certificate:

1. In the web interface, open the **Settings** → **Other** → **General** section.
2. Under **Core settings**, click the **Reissue** button for the **AI service certificate** setting.
3. Confirm certificate re-issue in the window that opens.
4. In the `/opt/kaspersky/mlservice/` directory, replace the certificate with a new certificate.
5. Restart the AI-rating and AI-status service of assets and the KUMA Core by using the command:

   ```
   systemctl restart mlservice
   ```

The new AI service certificate is applied.

Auditing and monitoring solution status

This section provides information on auditing and monitoring the status of Kaspersky SIEM.

Audit and monitoring of KUMA

KUMA audit and monitoring are used to assess the state of the deployed solution, identify potential infrastructure and configuration issues, and ensure stable component operation and correct event processing.

Audit and monitoring are performed sequentially and involve the following steps:

1 Technical audit

A technical audit is designed to check the infrastructure, configuration, and condition of KUMA components. This stage includes six basic steps:

1. Verifying resources and configuration

   Verify that the system is deployed correctly:

   - Verify that sufficient hardware resources are allocated.
   - Check the structure of the inventory file.
   - Check the distribution of service roles (storage, collector, correlator).

If necessary, check the dashboards to identify high-load components.

2. Analyzing the system state

   After verifying the system configuration, perform the current state analysis of KUMA:

   - Analyze the KUMA alerts from VictoriaMetrics.
   - Collect the log records using `getlogs` and check the microservices log records for errors.

3. Telemetry analysis

   Check key metrics:

   - Storage metrics:
     - Failed QPS
     - Failed Insert QPS
     - Delayed Insert QPS
     - Rejected Insert QPS
     - Distribution Queue
     - Failed Select QPS
     - Read-only Replicas
   - General metrics:
     - Load
     - CPU
     - Memory
     - Disk

4. Checking the fault tolerance

   Perform integral checks:

   - Controlled temporary shutdown of one of the active cluster nodes running a pod with KUMA Core.
   - Controlled temporary shutdown of one of the controllers.

5. Checking the cluster

   Check the following settings:

   - Synchronization of time between cluster nodes.
   - The uniqueness of the `/etc/machine-id` across the cluster nodes.
   - The validity of the cluster's internal certificates.

- Accessibility of the Metrics server from any cluster controller.
- The status of the KUMA Core volume and the Metrica service volume.
- Used disk space on the KUMA Core volume.

6. Checking the virtualization

   In the final step, verify the following:

   - The correct versions of hypervisors to host the virtual machines with KUMA Core cluster members are used.
   - Actions are not performed on running virtual machines (for example, taking snapshots, backups, or migrating them between servers).
   - Dynamic memory allocation is not used for virtual machines hosting KUMA Core cluster members.

After completing the technical audit, you can proceed to the functional audit.

2 Functional audit

At this stage, the correctness of KUMA usage as a SIEM system is assessed. This stage includes five main steps:

1. Checking the documentation

   Make sure that the documentation describes the following:

   - Maintenance processes.
   - Detection rule management.
   - Monitoring processes.

2. Analyzing event sources

   Check the following:

   - Inbound metrics by source type (average, peak, event size).
   - Coverage of event sources (number of devices).
   - Usage of event sources.
   - Issues with event sources normalization.
   - Comparison of event sources with recommendations (MITRE ATT&CK techniques).

3. Threshold analysis (detection rules)

Perform the following actions:

- Analysis of the list of thresholds.
- Analysis of threshold triggering statistics.
- Analysis of segmentation rules.

4. Testing integrations

   Make sure the following integrations are configured and working correctly:

   - Asset model.
   - Directory and name services (AD, DNS).
   - Sources of TI (Threat Intelligence).
   - GeoIP services.
   - External notifications (for example, NCIRCC).

5. Checking the processes

   Make sure that the following processes are configured and running correctly:

   - Role assignment.
   - Implementation of workflows.
   - Composition and classification of alerts and incidents.
   - Interaction with external systems, including NCIRCC.

   After completing the functional audit, proceed to setting up monitoring.

3 Configuring KUMA monitoring

Monitoring is used to continuously monitor the state of the system after an audit. It includes:

1. Business checks

   How to perform business checks

   Business checks help to make sure that the system collects events and generates alerts correctly. First, the collection and storage of events is checked, then their correlation in alerts.

Monitoring check

To verify that events are being received by the system:

1. Create and run a separate collector for monitoring.

   For example, at the **Transport** step, select the connector of the **HTTP** type, at the **Event parsing** step, select the **json** parsing method, and at the **Routing** step, select the **storage** type destination.

2. Send several test events at regular intervals with a unique value in one of the fields to the collector.

3. Find the event in ClickHouse via the KUMA REST API 15 seconds after sending the events.

If the check is successful, verify the status of the other checks. If the issue persists, contact Kaspersky Technical Support.

Correlation check

To check that events generate alerts correctly:

1. Add a test correlation rule of the simple type to one or more existing correlators.

   When creating a correlation rule, on the **Actions** tab, select the **Loop to correlator** check box.

2. In the previously created collector (at the monitoring check stage) on the **Routing** tab, add the correlator as a destination.

3. Send events that match the correlation rule selector at regular intervals.

4. After 30–60 seconds, check via the KUMA REST API whether an alert has been created, the **lastSeen** field updated, and the event count in the alert increased.

If the check is successful, verify the status of the other checks. If the issue persists, contact Kaspersky Technical Support.

2. Standard checks

   After conducting business checks, make sure that the following is monitored:

   - Operating system state: checking the operability of the operating system on which KUMA components are installed.
   - Network availability: checking the connection between devices on which KUMA components are installed, in accordance with the deployment scheme.
   - Web interface availability: checking if the KUMA web interface is working.

3. Atomic checks

   Types of atomic checks

   Atomic checks are performed for each KUMA service using VictoriaMetrics metrics, enabling detailed monitoring of the system state.

Check	Severity in case of failure	Description	Query example
Component status (Up/Down)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`up`
Processing EPS	Medium	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`rate(kuma_processing{job="kuma",serviceKind="<collector/correlator>",serviceN ame=~"<targe`
Errors of sending normalized events (destination) per second (Output Errors)	Medium	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`rate(kuma_outErrors{job="kuma",serviceKind="<collector/correlator>",serviceName=~"<t arget`
Output disk buffer size	Medium	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`kuma_destinationDiskBufferSize{job="kuma",serviceKind="<collector/correlator>",service Nam`
The number of lost events per second (Output Event Loss)	High	The check can be performed by querying the VictoriaMetrics store included in KUMA.	`rate(kuma_eventLoss{job="kuma",serviceKind="<collector/correlator>",serviceName=~"< target`
Number of normalization errors per second (Normalization Errors)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`rate(kuma_normalizationErrors{job="kuma",serviceKind="collector",serviceName=~"<tar get>"]`
Average server load for the last 1, 5 and 15 minutes (Load Average)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`max(kuma_load{job="kuma",serviceKind="<core/collector/correlator/storage>",serviceNa me=~'` `(hostname, kind`
Utilization of the host CPU (CPU total)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`max(kuma_cpuOS{job="kuma",serviceKind="<core/collector/correlator/storage>",service Name=~` `(hostname)`
Total host memory utilization (Memory total)	High	The check can be performed by querying the	`max(kuma_memOS{job="kuma",serviceKind="<core/collector/correlator/storage>",service Name=~` `(hostname)`

Check	Severity in case of failure	Description	Query example
		VictoriaMetrics store, which is part of KUMA.	
Host disk space utilization: `/` and `/opt/kaspersky/kuma` directories (Disk space)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`max(kuma_diskOS{job="kuma",serviceKind="<core/collector/correlator/storage>",service Name= (hostname, kind)`
Correlation rule rate limiter hits in one second	Medium	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`rate(kuma_correlationRateLimitReached{job="kuma",serviceKind="correlator",serviceNa me=~"<`
Total number of queries executed by the ClickHouse cluster (Active Queries)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`ClickHouseMetrics_Query{job="kumaclickhouse",serviceKind="clickhouse",serviceName=~"<targe`
Number of unsuccessful requests to add events to ClickHouse in one second (Failed inserts)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`rate(ClickHouseProfileEvents_FailedInsertQuery{job="kumaclickhouse",serviceKind="clickhous <target>"}[1m])`
Number of replicated tables in which writing is prohibited (Read-only Replicas)	High	The check can be performed by querying the VictoriaMetrics store, which is part of KUMA.	`ClickHouseMetrics_ReadonlyReplica{job="kumaclickhouse",serviceKind="clickhouse",serviceNam`

It is recommended to configure monitoring after completing the audit.

After configuring monitoring, check the following:

- Service availability.
- Receipt and storage of events.
- Generation of alerts.
- No loss of events.
- Correctness of metrics.

Monitoring the status of services

The KUMA solution is built on a microservice architecture. Each component of the solution, such as collectors, correlators, or storages, operates as a separate service. Therefore, the overall health of the solution is determined by the operational state of all its services. A number of tools for monitoring service status are available out of the box and do not require additional configuration. At the same time, you can manage some service status monitoring settings as you see fit. This will help pinpoint service issues that are specific to a particular solution configuration or an organization's infrastructure.

Built-in mechanisms for diagnosing service operation

One way to determine the current state of a service is its status. The service status is determined automatically based on the following information:

- Availability of the service
- Errors in the log files of the service
- Values of configurable settings

Possible service statuses

- Green means that the service is running and accessible from the KUMA Core server.
- Red means that the service is not running or is not accessible from the KUMA Core server.
- Yellow means that the service is running, but there are errors in the service log, or there are alerts for the service from Victoria Metrics. You can view the error message by hovering the mouse pointer over the service status. Yellow is the status that applies to all services except for the agent.
- Purple means that the service configuration file has changed, but no other errors are present. If a service has an incorrect configuration file and has errors, for example, from Victoria Metrics, status of the service is yellow.
- Gray means that an active service exists in the remote tenant and continues to run. Services with the gray status are kept when you delete the tenant to let you copy the ID and remove services on your servers. Only the General administrator can delete services with the gray status. When a tenant is deleted, the services of that tenant are assigned to the Main tenant.

When the service status changes, an audit event is generated. You can create search queries for audit events, create widgets based on such events, or use them in correlation rules.

Another tool for monitoring services is KUMA metrics, which provide dashboards with information about metrics and visualization of key parameters of various KUMA services. You can use this tool to monitor the status of all services except cold storage and agent. For example, using metrics, you can identify an insufficiency of allocated resources.

To gain access to KUMA metrics, users must have the appropriate role or access rights.

Configuring settings for monitoring service status

Only users with the General Administrator role can configure threshold values of KUMA service monitoring.

To configure the services:

1. In the web interface, open the **Settings** → **Other** → **Services monitoring** section.

2. Specify the values of monitoring parameters for the services.

   Service monitoring does not apply to cold storage.

   If you specify a value that does not fit the range or match the format, the value is reset to the previously configured value.

3. Click **Save**.

KUMA logs a Service monitoring thresholds changed audit event.

KUMA monitors the status of services in accordance with the specified parameters. If the specified thresholds are exceeded, the following changes occur:

- KUMA logs an audit event called Metrics alert is registered for service.

- KUMA sends a notification email message to the Main administrator.

- Services are displayed in the **Active services** section with a yellow status. If you hover over the status icon, an error message is displayed.

  To find services with errors, in the **Active services** section, you can filter services by statuses or enter a word from the error text, for example, `QPS` or `buffer`, in the search field and press **ENTER**. The following special characters are prohibited: `"`, `}`, `{`.

Examples of service status tracking

The following examples show how to monitor service status.

1. If the collector service has a yellow status in the **Active services** section and you see the **Enrichment errors increasing** message, you can:

   - Go to the **Metrics** → **<service type>** → **<service name>** → **Enrichment** → **Errors** section, find out which enrichment is causing errors, and view the chart to find out when the problem started and how it evolved.

   - Check the DNS or Kaspersky CyberTrace connection settings because one probable cause of enrichment errors is the unavailability of the DNS server or enrichment errors of Kaspersky CyberTrace.

2. If the collector service has a yellow status in the **Active services** section and you see the **Output Event Loss increasing** message, you can:

   - Go to the **Metrics** → **<service type>** → **<service name>** → **IO** → **Output Event Loss** section and view the chart to find out when the problem started and how it evolved.

   - Check whether the destination is available and connected correctly, or find out why the buffer size is exceeded, because a likely cause of loss of events is unavailability of a destination or a buffer overflowing.

Using correlation rules

To track the status of KUMA services, you can use correlation rules. To do this, you can download the [OOTB] KUMA package - RU or [OOTB] KUMA package - ENG correlation rule package from the repository; this package also includes correlation rules for monitoring the health of KUMA services. For example, this package includes the `R503_11_Alert for detecting possible performance issues in KUMA services` rule. As a result of this rule, KUMA creates an alert whenever a Metrics alert registered for the service audit event is generated.

Creating widgets and reports

To visualize the status of KUMA services, you can add widgets to the dashboard that are configured to display statistics on Metrics alert for the service is registered or Service status is changed audit events.

Disabling service monitoring

To disable service monitoring:

1. In the KUMA web console, go to the **Settings** → **Other** → **Services monitoring** section.

2. If you want to disable service monitoring for collectors only, in the **Collectors** section, select the **Disable connector errors** check box.

   This disables only the analysis of the **Connector errors** metric for collectors.

3. If you want to disable monitoring of all services, disable the **Status** toggle switch.

KUMA service monitoring is disabled, and services do not get the yellow status.

Viewing KUMA metrics

To monitor KUMA services, the flow of events from sources and correlations, KUMA collects and stores a large amount of *metrics* data. The Metrics service (the VictoriaMetrics time series database) is used to collect, store, and analyze this data.

Metrics are available on KUMA services at all times and are collected every 15 seconds. If the KUMA service is unavailable, changes that are multiples of `<duration of unavailability> / <collection interval>` become lost.

Information about metrics and visualization of key parameters of various KUMA services is presented on dashboards in the **Metrics** section. The collected metrics are visualized using the Grafana solution.

To learn more about the Grafana dashboards, watch this video:

https://www.youtube.com/watch?v=WH-gdCngiJs

Selecting the **Metrics** section opens the automatically updated Grafana portal deployed as part of KUMA Core installation process.

How to determine the host the KUMA Core is installed on

To determine on which host the Core is running, run the following command in the terminal of one of the controllers:

```
k0s kubectl get pod -n kuma -o wide
```

The KUMA Core service configures VictoriaMetrics and Grafana automatically, user participation is not required. Graphs in the **Metrics** section appear with a delay of approximately 1.5 minutes. If the **Metrics** section shows `core:<port number>`, this means that the metrics were received from the host where the KUMA Core was installed. In other configurations, the name of the host from which KUMA receives metrics is displayed.

Collector metrics

IO—metrics related to the service input and output

Metric name	Description
Processing EPS	Number of events processed per second. Starting with KUMA 4.2, the Processing EPS counter takes into account both the auditd event parts and the final (collated) event. For this reason, the **Processing EPS** metric can increase.
Output EPS	Number of events per second sent to the destination.
Output Latency	The time in milliseconds that passed while sending an event packet and receiving a response from the destination. The median value is displayed.
Output Errors	The number of errors occurring per second while sending event packets to the destination. Network errors and errors writing to the disk buffer of the destination are displayed separately.
Output Event Loss	Number of events lost per second. Events can be lost due to network errors or errors writing the disk buffer of the destination. Events are also lost if the destination responds with an error code, for example, in case of an invalid request.
Output Disk Buffer Size	The size of the disk buffer of the collector associated with the destination, in bytes. If a zero value is displayed, no event packets have been placed in the collector's disk buffer and the service is operating correctly.

Metric name	Description
Write Network BPS	The number of bytes received into the network per second.
Connector errors	The number of errors in the connector logs.

Normalization—metrics related to the normalizers

Metric name	Description
Raw & Normalized event size	The size of the raw event and size of the normalized event. The median value is displayed.
Errors	The number of normalization errors per second.

Filtration—metrics related to filters

Metric name	Description
EPS	The number of events per second sent to be processed. If a filter is present in the configuration of the collector service, events that meet the filter conditions are discarded, and only events that do not meet these conditions are sent for processing.

Aggregation—metrics related to the aggregation rules

Metric name	Description
EPS (events per second)	The number of events received and generated by the aggregation rule per second. This metric helps determine the effectiveness of aggregation rules.
Buckets	The number of buckets in the aggregation rule.

Enrichment—metrics related to enrichment rules

Metric name	Description
Cache RPS	The number of requests per second to the local cache.
Source RPS	The number of requests per second to an enrichment source. Data is collected only for the **dns** and **cybertrace** enrichment source types.
Source Latency	Time in milliseconds passed while sending a request to the enrichment source and receiving a response from it. The median value is displayed.
Queue	The size of the enrichment request queue. This metric helps to find bottleneck enrichment rules.
Errors	The number of errors per second while sending requests to the enrichment source.

Process—metrics related to processes

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.

Correlator metrics

IO—metrics related to the service input and output

Metric name	Description
Processing EPS	Number of events processed per second.
Output EPS	Number of events per second sent to the destination.
Output Latency	The time in milliseconds that passed while sending an event packet and receiving a response from the destination. The median value is displayed.
Output Errors	The number of errors occurring per second while sending event packets to the destination. Network errors and errors writing to the disk buffer of the destination are displayed separately.
Output Event Loss	Number of events lost per second. Events can be lost due to network errors or errors writing the disk buffer of the destination. Events are also lost if the destination responds with an error code, for example, in case of an invalid request.
Output Disk Buffer Size	The size of the disk buffer of the collector associated with the destination, in bytes. If a zero value is displayed, no event packets have been placed in the collector's disk buffer and the service is operating correctly.
Write Network BPS	Number of bytes transmitted into the network per second.

Correlation—metrics related to correlation rules

Metric name	Description
EPS	The number of correlation events per second generated by the correlation rule.
Buckets	The number of buckers in a correlation rule of the standard type.
Rate Limiter Hits	The number of times the correlation rule exceeded the rate limit per second.
Active Lists OPS	The number of operations requests per second sent to the active list, and the operations themselves.
Active Lists Records	The number of records in the active list.
Active Lists On-Disk Size	The size of the active list on the disk, in bytes.
Context Tables OPS	Number of queries to the context table in 1 second with the operation indicated.
Context Tables Records	Current number of records in the context table
Context Tables On-Disk Size	Current size of context table on disk.

Enrichment—metrics related to enrichment rules

Metric name	Description
Cache RPS	The number of requests per second to the local cache.
Source RPS	The number of requests per second to an enrichment source, such as a dictionary.
Source Latency	Time in milliseconds passed while sending a request to the enrichment source and receiving a response from it. The median value is displayed.

Metric name	Description
Queue	The size of the enrichment request queue. This metric helps to find bottleneck enrichment rules.
Errors	The number of errors per second while sending requests to the enrichment source.

Response—metrics associated with response rules

Metric name	Description
RPS	The number of times a response rule was activated per second.

Process—metrics related to processes

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.

Storage metrics

IO—metrics related to the status of ClickHouse cluster nodes

Metric name	Description
Output EPS	Number of events per second that were inserted into the ClickHouse node or into the disk buffer of the node.
Output Latency	Latency of inserting a batch either into the ClickHouse node or into the disk buffer of the node.
Output Errors	Number of errors per second when inserting a batch into the ClickHouse node or into the disk buffer of the node.
Output Disk Buffer Size	Size of the disk buffer of the ClickHouse node.
Output Event Loss	Number of events that were permanently lost on each ClickHouse node.
Batch size	The size of the batch of events to be inserted into the ClickHouse node.
Insert interval 5min Q1	Duration of the first quartile of the event insertion interval for the last 5 minutes.

ClickHouse / General—metrics related to the general settings of the ClickHouse cluster

Metric name	Description
Active Queries	The number of active queries sent to the ClickHouse cluster. This metric is displayed for each ClickHouse instance.
QPS	The number of queries per second sent to the ClickHouse cluster.

Metric name	Description
Failed QPS	The number of failed queries per second sent to the ClickHouse cluster.
Allocated memory	The amount of RAM allocated to the ClickHouse process (depends on the specifications of the server and can be expressed, for example, in GB or MB).
Active parts	The number of active parts. Active parts are data (files on disk) that are currently being used to process queries.
Detached parts (count)	The number of detached (disconnected) parts. Detached parts are data that exists on disk, but do not participate in file read and write operations.
Detached parts (size)	Disk space taken up by detached parts. You can specify the maximum size of detached parts in the range from 1% to 90%. The default setting is 1%. If the size of detached parts exceeds the specified maximum value, KUMA assigns the yellow status to the running storage service in the **Active services** section.

ClickHouse / Insert—metrics related to inserting events into a ClickHouse instance

Metric name	Description
Insert EPS	The number of events per second inserted into the ClickHouse instance.
Insert QPS	The number of ClickHouse instance insert queries per second sent to the ClickHouse cluster. If the **Insert QPS** metric demonstrates a growing queue of queries and the metric is greater than 1, we recommend also looking at the **Batch size** metric value to adjust the storage buffering settings in the settings of the storage service configuration. Example: The **Insert QPS** metric is greater than 1 and equals 8. The **Batch size** metric is 1.2 GB (in bytes). In this case, you can find the buffer size by multiplying **Insert QPS** by **Batch size**: 8 * 1.2 = 9.6 GB. Round the resulting value of 9.6 and specify it in bytes (for example, 10000000000 bytes) as the **Buffer size** setting on the **Advanced settings** tab of the storage service configuration. Also specify a **Buffer flush interval** of 2 seconds. Increasing the buffer size and buffer flush interval will help relieve the query queue. Normally, the **Insert QPS** metric should be less than 1.
Failed Insert QPS	The number of failed ClickHouse instance insert queries per second sent to the ClickHouse cluster.
Delayed Insert QPS	The number of delayed ClickHouse instance insert queries per second sent to the ClickHouse cluster. Requests were delayed by the ClickHouse node due to exceeding the soft limit on active merges.
Rejected Insert QPS	The number of rejected ClickHouse instance insert queries per second sent to the ClickHouse cluster. Requests were rejected by the ClickHouse node due to exceeding the hard limit on active merges.
Active Merges	The number of active merges.
Distribution Queue	The number of temporary files with events that could not be inserted into the ClickHouse instance because it was unavailable. These events cannot be found using search.

ClickHouse / Select—metrics related to event selections in the ClickHouse instance

Metric name	Description
Select QPS	The number of ClickHouse instance event select queries per second sent to the ClickHouse cluster.
Failed Select QPS	The number of failed ClickHouse instance event select queries per second sent to the ClickHouse cluster.

ClickHouse / Replication—metrics related to replicas of ClickHouse nodes

Metric name	Description
Active Zookeeper Connections	The number of active connections to the Zookeeper cluster nodes. In normal operation, this number should be equal to the number of nodes in the Zookeeper cluster.
Read-only Replicas	The number of read-only replicas of ClickHouse nodes. In normal operation, no such replicas of ClickHouse nodes must exist.
Active Replication Fetches	The number of active processes of downloading data from the ClickHouse node during data replication.

Metric name	Description
Active Replication Sends	The number of active processes of sending data to the ClickHouse node during data replication.
Active Replication Consistency Checks	The number of active data consistency checks on replicas of ClickHouse nodes during data replication.

ClickHouse / Networking—metrics related to the network of the ClickHouse cluster

Metric name	Description
Active HTTP Connections	The number of active connections to the HTTP server of the ClickHouse cluster.
Active TCP Connections	The number of active connections to the TCP server of the ClickHouse cluster.
Active Interserver Connections	The number of active service connections between ClickHouse nodes.

Agents

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.
Disk used (events)	Percentage of /opt filled with events.
Disk used (except events)	Percentage of /opt filled with data other than events.

KUMA Core metrics

Raft—metrics related to reading and updating the state of the KUMA Core

Metric name	Description
Lookup RPS	Number of lookup procedure requests per second sent to the KUMA Core, and the procedures themselves.
Lookup Latency	Time in milliseconds spent running the lookup procedures, and the procedures themselves. The time is displayed for the 99th percentile of lookup procedures. One percent of lookup procedures may take longer to run.
Propose RPS	Number of Raft (SQLite) propose procedure requests per second sent to the KUMA, and the procedures themselves.
Propose Latency	Time in milliseconds spent running the Raft (SQLite) propose procedures, and the procedures themselves. The time is displayed for the 99th percentile of propose procedures. One percent of propose procedures may take longer to run.

Data mining—metrics related to data collection and analysis

Metric name	Description
Executing Rules	Number of running schedulers for executing data collection and analysis requests.
Queued Rules	Number of schedulers for executing queued data collection and analysis requests.
Execution Errors	Number of errors that occurred when running the data collection and analysis scheduler.
Execution Latency	How long takes a scheduler to execute requests.

Tasks—metrics related to monitoring the running of tasks on the KUMA Core

Metric name	Description
Active tasks	Number of tasks run per unit time.
Task Execution latency	Duration of running tasks in seconds.
Errors	Number of errors when running tasks.

API—metrics related to API requests

Metric name	Description
RPS	Number of API requests made to the KUMA Core per second.
Latency	Time in milliseconds spent processing a single API request to the KUMA Core. The median value is displayed.
Errors	Number of errors per second while sending API requests to the KUMA Core.

Notification Feed—metrics related to user activity.

Metric name	Description
Subscriptions	Number of clients connected to the KUMA Core via SSE to receive server messages in real time. This number is normally equal to the number of clients that are using the KUMA web interface.
Errors	Number of errors per second while sending notifications to users.

Schedulers—metrics related to KUMA Core tasks

Metric name	Description
Active	The number of repeating active system tasks. The tasks created by the user are ignored.
Latency	The time in milliseconds spent running the task. The median value is displayed.
Errors	Number of errors that occurred per second while performing tasks.
Alerts Queue	Number of alerts in the queue for insertion into the database.

IO—metrics related to the status of KUMA Core nodes

Metric name	Description
Output Disk Buffer Size	The size of each of disk file buffer on the KUMA Core node for the tasks for sending audit events, monitoring, collecting and analyzing data for correlators.

Process—metrics related to processes

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.

Metric name	Description
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.

KUMA agent metrics

IO—metrics related to the service input and output

Metric name	Description
Processing EPS	Number of events processed per second.
Output EPS	Number of events per second sent to the destination.
Output Latency	The time in milliseconds that passed while sending an event packet and receiving a response from the destination. The median value is displayed.
Output Errors	The number of errors occurring per second while sending event packets to the destination. Network errors and errors writing to the disk buffer of the destination are displayed separately.
Output Event Loss	Number of events lost per second. Events can be lost due to network errors or errors writing the disk buffer of the destination. Events are also lost if the destination responds with an error code, for example, in case of an invalid request.
Output Disk Buffer Size	The size of the disk buffer of the collector associated with the destination, in bytes. If a zero value is displayed, no event packets have been placed in the collector's disk buffer and the service is operating correctly.
Write Network BPS	The number of bytes received into the network per second.

Process—metrics related to processes

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.

Metric name	Description
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.

Event router metrics

IO—metrics related to the service input and output

Metric name	Description
Processing EPS	Number of events processed per second.
Output EPS	Number of events per second sent to the destination.
Output Latency	The time in milliseconds that passed while sending an event packet and receiving a response from the destination. The median value is displayed.
Output Errors	The number of errors occurring per second while sending event packets to the destination. Network errors and errors writing to the disk buffer of the destination are displayed separately.
Output Event Loss	Number of events lost per second. Events can be lost due to network errors or errors writing the disk buffer of the destination. Events are also lost if the destination responds with an error code, for example, in case of an invalid request.
Output Disk Buffer Size	The size of the disk buffer of the collector associated with the destination, in bytes. If a zero value is displayed, no event packets have been placed in the collector's disk buffer and the service is operating correctly.
Write Network BPS	The number of bytes received into the network per second.

Process—metrics related to processes

Metric name	Description
Memory	RAM usage (RSS) in megabytes.
Disk BPS	The number of bytes read from or written to the disk per second.
Network BPS	The number of bytes received/transmitted over the network per second.
Network Packet Loss	The number of network packets lost per second.
GC Latency	The time, in milliseconds, spent executing a GO garbage collection cycle The median value is displayed.
Goroutines	The number of active goroutines. This number is different from the operating system's thread count.

OS—metrics related to the operating system.

Metric name	Description
Load	Average load.
CPU	CPU load as a percentage.
Memory	RAM usage (RSS) as a percentage.
Disk	Disk space usage as a percentage.

Metrics of the Metrics service

Stats

Metric name	Description
Version	KUMA version.
Total Datapoints	Total number of data points in the database.
Ingestion rate	Database insert rate (data points per second).
Read requests	Database select rate
Available CPU	Available CPU core count
Uptime	Uptime of the service.
Active series	Number of active time series.
Disk space usage	Disk space occupied.
Available memory	Memory available on the server.
Bytes per point	Average data point size (in bytes).

Overview

Metric name	Description
Datapoints ingestion rate	Database insert rate (data points per second).
Requests rate	HTTP request rate by path.
Active timeseries	Number of active time series.
Query duration 0.99 quantile	Query execution time (99th percentile).
Requests error rate	HTTP request error rate.

Resource usage

Metric name	Description
RSS memory % usage	RSS memory usage (percent).
RSS anonymous memory % usage	Anonymous RSS memory usage (percent).
Memory usage	Memory usage (heap, resident, system).
CPU % usage	CPU load (percent).
Open FDs	File descriptor usage.
CPU	CPU core usage.
Goroutines	Number of Go goroutines.
Disk writes/reads	Disk read and write rate (bytes/s).
Threads	Number of threads.
Disk write/read calls	Number of I/O system calls.
TCP connections rate	Rate of TCP connection creation.
TCP connections	Active TCP connections.
Network usage	Network traffic (inbound/outbound).
CPU spent on GC	CPU time spent on garbage collection.

Metric name	Description
Go scheduling latency	Latency of the Go scheduler.
Slow inserts %	Number of slow inserts (percent).

Troubleshooting

Metric name	Description
Churn rate	Rate of appearance of new time series and disappearance of old time series.
Assisted merges	Forced merges, which are performed synchronously in the data writing thread when background merge processes cannot catch up with the accumulation of LSM tree parts.
Slow queries rate	Rate of slow queries.
Cache miss ratio	Number of cache misses when looking up data points (percent).
Cache usage % by type	Cache usage by type.
Deduplication rate	Data deduplication rate.
Samples dropped for last 1h	Deleted data points over the last hour.
Restarts	Number of service restarts.

Storage

Metric name	Description
Datapoints ingestion rate	Data point insert rate (data points per second).
Disk space usage - datapoints	Disk space occupied by data points.
Storage full ETA	Estimate of when storage will fill up.
Pending data points	Number of data points waiting to be written.
Datapoints	Number of data points by storage type.
LSM parts max by type	Maximum number of LSM tree parts by type.
Rows ignored for last 1h	Number of rows ignored over the last hour.
Active merges	Number of active merges.
Concurrent flushes on disk	Concurrent disk writes.
Merge speed	Data merge speed.
Series read per query	Average number of series per query.
Datapoints read per series	Average number of data points per series.
Datapoints read per query	Average number of data points per query.
Datapoints scanned per query	Number of data points scanned per query.

Alerting

Metric name	Description
Config error	Misconfiguration status.
Errors	Error rate according to alerting rules.
Alerting rules	Number of alerting rules.
Alerts fired total	Total number of alerts fired.
Top 10 groups by evaluation duration	Top 10 groups of alerting rules by execution time.
Rules execution rate	Rate of alerting rule execution.

Metric name	Description
Rules execution errors	Errors during execution of alerting rules.
Missed evaluations	Missed alert rule evaluations.
Top 10 active alerts	Top 10 active alerts by alerting rules.

Tenant metrics

Tenants Overview—metrics related to tenants

Metric name	Description
Tenant EPS (events per second according to license conditions)	Number of events per second received within the tenant.

KUMA metrics storage period

KUMA operation data is stored for three months by default. This storage period can be changed.

To change the storage period for KUMA metrics:

1. Log in to the server OS where the KUMA Core is installed.
2. In the file `/etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service`, in the `ExecStart` parameter, specify the required period by changing the following flag:

   ```
   --retentionPeriod=<metrics retention period in months>
   ```

   For example, if you want metrics to be stored for four months, specify the following:

   ```
   --retentionPeriod=4
   ```

3. Restart KUMA by running the following commands in sequence:

   ```
   systemctl daemon-reload
   systemctl restart kuma-victoria-metrics
   ```

   The storage period for metrics will be changed.

KUMA metric alert triggering conditions

If the value of a KUMA metric for a service exceeds the threshold of the corresponding parameter configured in the **Services monitoring** section, VictoriaMetrics sends an alert, and an error message is displayed in the status of that service.

Alerts are received from VictoriaMetrics at the following intervals:

- VictoriaMetrics collects information from KUMA services every 15 seconds.
- VictoriaMetrics updates alerts for KUMA services every minute.
- The KUMA Core service collects information from VictoriaMetrics every 15 seconds.

Thus, the total delay before a service status is updated is less than 2–3 minutes.

If you disabled the receipt of alerts from VictoriaMetrics, some KUMA services may still be displayed with a yellow status. This can happen in the following cases:

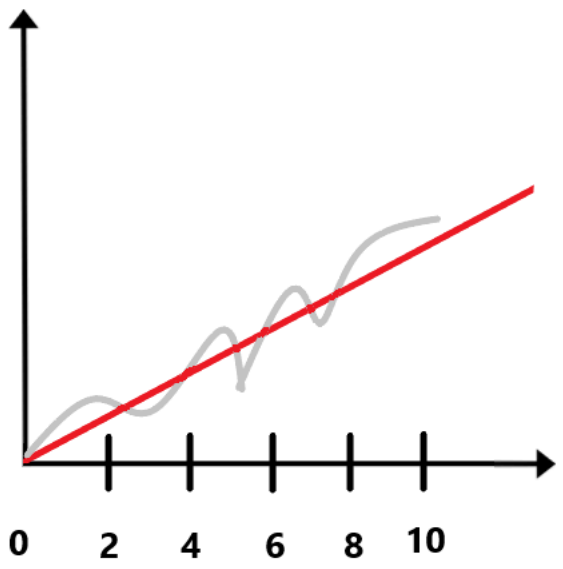
- For a storage service:
  - If an alert was received in response to an API request in the /status parameter from ClickHouse
  - If cold storage of the Storage service is not being monitored
- For a collector service: If an alert was received in response to an API request in the /status parameter.
- For a correlator service: If a response rule exists that requires the Advanced Responses module, but this module is not covered by the current license, or the license that covers this module has expired.

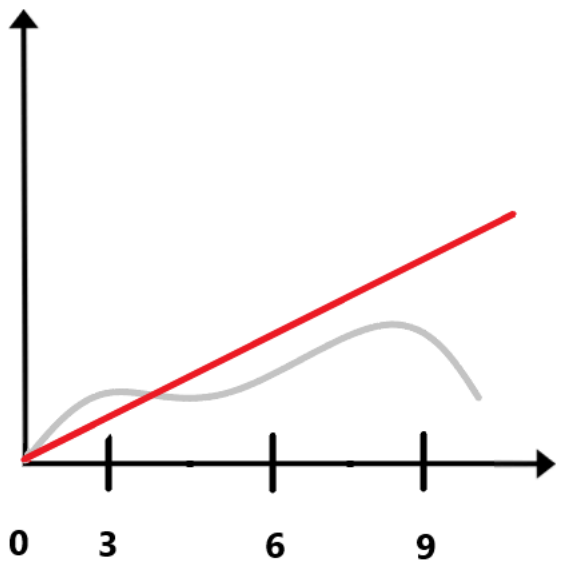
The table below provides information on which error messages may appear in the service status when an alert is received from VictoriaMetrics, and which metrics and parameters they are based on and in what way. For details on KUMA metrics that can trigger VictoriaMetrics alerts, see Viewing KUMA metrics.

For example, if the **Active services** table for a service displays a yellow status and the `High distribution queue` error message (the "Error message" column in the table below), you can view the information in the **Enrichment** widget, the **Distribution Queue** metric (the "KUMA metrics" column in the table below).

Description of error messages for KUMA services

Error message	Configurable alert parameters	KUMA metric	Description
`QPS threshold reached`	**QPS interval/window, minutes** **QPS Threshold**	Clickhouse / General → Failed QPS	An error message is displayed if the Failed QPS metric exceeds the specified **QPS Threshold** value for the duration specified by the **QPS interval/window, minutes** parameter. For example, if 25 out of 100 requests from VictoriaMetrics to the service were unsuccessful, and the **QPS Threshold** is 0.2, the alert is calculated as follows: (25 / 100) * 100 > 0.2 * 100 25% > 20% Because the percentage of unsuccessful requests is greater than the specified threshold, an error message is displayed for the service.
`Failed Insert QPS threshold reached`	**Failed insert QPS calculation interval/window, minutes** **Insert QPS threshold**	Clickhouse / Insert → Failed Insert QPS	An error message is displayed if the Failed Insert QPS metric exceeds the specified **QPS Insert Threshold** value for the duration specified by the **Failed Insert QPS calculation interval/window, minutes** parameter. For example, if 25 out of 100 requests from VictoriaMetrics to the service were unsuccessful, and the **QPS Insert Threshold** is 0.2, the alert is calculated as follows: (25 / 100) * 100 > 0.2 * 100 25% > 20% Because the percentage of unsuccessful requests is greater than the specified threshold, an error message is displayed for the service.

Error message	Configurable alert parameters	KUMA metric	Description
`High distribution queue`	**Distribution queue threshold** **Distribution queue calculation interval/window, minutes**	Clickhouse / Insert → Distribution Queue	An error message is displayed if the Distribution Queue metric exceeds the specified **Distribution queue threshold** value for the duration specified by the **Distribution queue calculation interval/window, minutes** parameter.
`Low disk space`	**Free space on disk threshold**	OS → Disk	An error message is displayed if the amount of free disk space (as a percentage) indicated by the Disk metric value is less than the value specified in the **Free disk space threshold** parameter. For example, an error message is displayed if the partition on which KUMA is installed takes up all the disk space.
`Low disk partition space`	**Free space on partition threshold**	OS → Disk	An error message is displayed if the amount of free space (as a percentage) on the disk partition that KUMA is using is less than the value specified in the **Free space on partition threshold** parameter. For example, an error message is displayed in the following cases: • If KUMA is installed in a high availability configuration, when the disk is mounted as a volume. • If the disk is mounted under /opt.
`Output Event Loss increasing`	**Output Event Loss**	IO → Output Event Loss	An error message is displayed if the Output Event Loss metric has been increasing for one minute. You can enable or disable the display of this error message using the **Output Event Loss** parameter.
`Disk buffer size increasing`	**Disk buffer increase interval/window, minutes**	IO → Output Disk Buffer SIze	An error message is displayed if the Output Disk Buffer Size metric monotonically increases for 10 minutes with the sampling interval specified by the **Disk buffer increase interval/window, minutes** parameter. For example, if the **Disk buffer increase interval/window, minutes** is set to 2 minutes, an error message is displayed if the disk buffer size has monotonically increased for 10 minutes with a sampling interval of 2 minutes (see the figure below). 

Error message	Configurable alert parameters	KUMA metric	Description
`High enrichment queue`	**Growing enrichment queue interval/window, minutes**	Enrichment → Queue	An error message is displayed if the Queue metric monotonically increases for 10 minutes with the sampling interval specified by the **Growing enrichment queue interval/window, minutes** parameter. For example, if the value of the **Growing enrichment queue interval/window, minutes** is 3, an error message is displayed if the enrichment queue has monotonically increased every 10 minutes with a sampling interval of 3 minutes. In the case shown in the figure below, the error message is not displayed because at the ninth minute the value of the metric decreased instead of increasing monotonically. 
`Enrichment errors increasing`	**Enrichment errors**	Enrichment → Errors	An error message is displayed if the Errors metric has been increasing for one minute. You can enable or disable the display of this error message using the **Enrichment errors** parameter.
`Connector log errors increasing`	**Disable connector errors**	IO → Connector Errors	An error message is displayed if the Connector Errors metric has been increasing between consecutive polls of the metric by VictoriaMetrics for one minute. You can enable or disable the display of this error message using the **Disable connector errors** parameter.

Migrating the Metrics service to another host

You can install the Metrics service using the `expand.sh` installer and the `expand.inventory.yml` inventory file.

Starting with KUMA 4.2, during the initial installation of the solution, the Metrics service is installed on the host specified in the `kuma_metrics` section of the inventory file. You can specify a different host to install the Metrics service. In any KUMA configuration, only one Metrics service must exist. When upgrading from KUMA 4.0 to 4.2, you must specify the host on which the active Metrics service is running in the `kuma_metrics` section of the inventory file. When the update starts, a check is performed, and if the Metrics service is not found on the specified host, an error is returned and the update is stopped.

In a high-availability configuration of KUMA, the Metrics service communicates with the available KUMA Core directly, bypassing the balancer.

If a Metrics service had been used, and after its removal a new service was installed, historical data is not deleted. The data of the Metrics service remains in the `/opt/kaspersky/kuma/metrics/<ID of the old Metrics service instance>/data` directory. You can stop the service and move data to another host, as well as replace the existing `data` directory with the transferred directory.

To install the Metrics service on another host:

1. Make sure the target machines satisfy the hardware and software requirements.

2. On the control computer, go to the directory with the extracted KUMA installer by running the following command:

```
cd kuma-ansible-installer
```

3. Create an inventory file named `expand.inventory.yml` by copying the `expand.inventory.yml.template` file:

```
cp expand.inventory.yml.template expand.inventory.yml
```

4. Edit the `expand.inventory.yml` inventory file and specify the host on which you want to install the Metrics service in the `kuma_metrics` section.

5. On the control computer, run the following command as root from the directory with the unpacked installer:

```
./expand.sh expand.inventory.yml
```

   This command creates files for creating and installing the Metrics service on the host specified in the `kuma_metrics` section.

6. In the web interface, open the **Resources and services** → **Active services** section, and in the **Add** drop-down list, select **Add metrics**.

7. In the window that is displayed, in the **Metrics service name** field, specify the name of the service.

8. Click **Add**.

   The window is closed and you are taken to the **Active services** section. The Metrics service has been added to the table and has the red status.

9. Copy the ID of the Metrics service. To do so, in the **Active services** section, select the check box next to the Metrics service and in the toolbar or the menu (⋮), click **Copy ID**.

10. Install the Metrics service on the host specified in the `expand.inventory.yml` inventory file. To do this, run the following command in the console:

```
sudo /opt/kaspersky/kuma/kuma metrics --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --api.port <API_port> --install
```

   where:

   - <FQDN> is the fully qualified domain name of the KUMA Core server.

   - <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).

- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` option is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

- <service_ID> is the service ID copied from the KUMA web interface.

- <API_port> is the port used for communication with the component being installed.

Example

```
sudo /opt/kaspersky/kuma/kuma metrics --core https://kuma.example.com:7210 --pair.fingerprint
d183f1208ca739e247997991403676a037dd64e34a5eb5ed59f83e54dc6e5145 --id XXXX --api.port YYYY --install
```

11. If you want to migrate the historical data of the old Metrics service, copy the `data` directory from the old host to the new one, preserving all file attributes (owner, group, access permissions, timestamps):

```
sudo mv /opt/kaspersky/kuma/metrics/<former_metrics_ID>/data /opt/kaspersky/kuma/metrics/<new_metrics_ID>/data
```

where:

- <former_metrics_ID> is the ID of the old Metrics service.

- <new_metrics_ID> is the ID of the new Metrics service.

After copying, make sure that the `data` directory and the files it contains are owned by the user and group of the Metrics service (by default, `kuma:kuma`):

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/metrics/<new_metrics_ID>/data
sudo chmod -R 750 /opt/kaspersky/kuma/metrics/<new_metrics_ID>/data
```

12. Start the Metrics service by running the following command:

```
sudo systemctl start metrics.service
```

The Metrics service is installed and running.

Integrity check of KUMA files

You can manually check the integrity of KUMA components using a suite of scripts based on the integrity_checker tool and located in the `/opt/kaspersky/kuma/integrity/bin` directory. An integrity check uses manifest XML files from the `/opt/kaspersky/kuma/integrity/manifest/*` directory, protected by a Kaspersky cryptographic signature.

Running the scripts requires a user account with permissions at least matching those of the KUMA account.

The integrity check tool processes each KUMA component individually, and it must be run on servers that has the appropriate components installed. An integrity check also checks the XML file that was used.

To check the integrity of component files:

1. Run the following command to navigate to the directory that contains the set of scripts:

```
cd /opt/kaspersky/kuma/integrity/bin
```

2. Depending on which KUMA component you want to check the integrity of, run one of the following commands:

```
KUMA Core and Storage components
```

```
./check_all.sh
```

```
KUMA Core component
```

```
./check_core.sh
```

```
KUMA collector component
```

```
./check_collector.sh
```

```
Storage component
```

```
./check_storage.sh
```

```
Event router component
```

```
./check_event_router.sh
```

```
KUMA Agent for Windows
```

```
./check_kuma_exe.sh <full path to kuma.exe omitting file name>
```

The standard location of the agent executable file on the Windows device is `C:\Program Files\Kaspersky Lab\KUMA\`.

```
KUMA Agent for Linux
```

```
./check_linux_agent.sh full path to the executable file of the KUMA agent without the file name>.
```

The integrity of the component files is checked.

The result of checking each component is displayed in the following format:

- The Summary section describes the number of scanned objects along with the scan status: integrity not confirmed / object skipped / integrity confirmed:
  - Manifests – the number of manifest files processed.
  - Files – the number of KUMA files processed.
  - Directories – not used when KUMA integrity checking is performed.
  - Registries – not used when KUMA integrity checking is performed.
  - Registry values – not used when KUMA integrity checking is performed.
- Component integrity check result:
  - SUCCEEDED – integrity confirmed.
  - FAILED – integrity violated.

Uninstalling the solution

To uninstall the solution, use the Ansible tool and the inventory file that you have prepared.

To uninstall a solution:

1. On the control computer, go to the installer directory:

   ```
   cd kuma-ansible-installer
   ```

2. Execute the following command:

   ```
   ./uninstall.sh <inventory file>
   ```

   KUMA and all of its data is removed from the server.

The databases that were used by KUMA (for example, the ClickHouse storage database) and the data therein must be deleted separately.

Special considerations for removing a high availability configuration of KUMA

Which components need to be removed depends on the value of the `deploy_to_k8s` parameter in the inventory file that you are using to remove KUMA:

- If the setting is `true`, the Kubernetes cluster created during the KUMA installation is deleted.
- If the setting is `false`, all KUMA components except for the Core are removed from the Kubernetes cluster. The cluster is not deleted.

In addition to the KUMA components installed outside the cluster, the following directories and files are deleted on the cluster nodes:

- /usr/bin/k0s
- /etc/k0s/
- /var/lib/k0s/
- /usr/libexec/k0s/
- ~/k0s/ (for the ansible_user)
- /opt/longhorn/
- /opt/cni/
- /opt/containerd

When a cluster is being deleted, error messages may appear, however, it does not interrupt the installer.

- You can ignore such messages for the **Delete KUMA transfer job** and **Delete KUMA pod** tasks.
- For the **Reset k0s** task (if an error message contains the following text: `To ensure a full reset, a node reboot is recommended.`) and the Delete k0s Directories and files task (if an error message contains the following text: `I/O error: '/var/lib/k0s/kubelet/plugins/kubernetes.io/csi/driver.longhorn.io/`), we recommend restarting the relevant host and trying to remove KUMA again with the same inventory file.

After removing KUMA, restart the hosts on which the KUMA or Kubernetes components were installed.

Collecting and enriching events

This section describes how to configure the receipt, processing, and enrichment of events for further analysis.

Connect event sources

This section provides information on configuring the receipt of events from various sources.

Kaspersky

This section describes how to configure the receiving of events from Kaspersky products that are used for security monitoring and integration with the KUMA SIEM system.

Kaspersky Security Center (Administration server)

Configuring the receiving and transferring of events from the Administration Server of Kaspersky Security Center to Kaspersky SIEM consists of the following steps:

1. Configuring Kaspersky Security Center event export

Kaspersky Security Center allows you to configure the settings for exporting events in the CEF format to a SIEM system.

> The function of exporting Kaspersky Security Center events in the CEF format to SIEM systems is available with Kaspersky Endpoint Security for Business Advanced license or above.

1. In Kaspersky Security Center console tree, select the **Administration server** node.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select **Configure export to SIEM system** from the drop-down list.

   The **Properties: Events** window opens. By default the **Events export** section is displayed.
4. In the **Events export** section, select the **Automatically export events to SIEM system database** check box.
5. In the **SIEM system** drop-down list select **ArcSight (CEF format)**.

6. In the corresponding fields, specify the address of the KUMA SIEM system server and the port for connecting to the server. Select **TCP/IP** as the protocol.

   You can click **Export archive** and specify the starting date from which pre-existing KUMA events are to be exported to the SIEM system database. By default, Kaspersky Security Center exports events starting from the current date.

7. Click **OK**.

Kaspersky Security Center Administration Server automatically exports all events to Kaspersky SIEM.

❷ Configuring the KUMA collector for Kaspersky Security Center event reception

After configuring the export of events in the CEF format from Kaspersky Security Center Administration Server, configure the collector in the Kaspersky SIEM web interface.

1. In the KUMA web interface, select **Resources** → **Collectors**.

2. In the list of collectors, find the collector with the **[OOTB] KSC** normalizer and open it for editing.

3. At the **Transport** step, in the **URL** field, specify the port to be used by the collector to receive Kaspersky Security Center events.

   The port must match the port of the KUMA SIEM system server.

4. At the **Event parsing** step, make sure that the **[OOTB] KSC** normalizer is selected.

5. At the **Routing** step, make sure that the following destinations are added to the collector resource set:

   - **Storage**. To send processed events to the storage.

   - **Correlator**. To send processed events to the correlator.

   If the **Storage** and **Correlator** destinations were not added, create them.

6. At the **Setup validation** tab, click **Create and save service**.

7. Copy the command for installing the KUMA collector that appears.

❸ Installing the KUMA collector in the network infrastructure

After configuring the collector for obtaining Kaspersky Security Center events in the CEF format, you need to install the KUMA collector on the server of the network infrastructure intended for reception of events.

❹ Verifying receipt of Kaspersky Security Center events by the KUMA collector

You can verify if the events from Kaspersky Security Center Administration Server were correctly exported to the KUMA SIEM system by using the KUMA web interface to search for related events.

To display Kaspersky Security Center events in the table, enter a search expression.

Example

```
SELECT
    Timestamp,
    Severity,
    Message
FROM events
WHERE DeviceProduct = 'KSC'
ORDER BY Timestamp DESC
LIMIT 250
```

Kaspersky Security Center (MS SQL)

Configuring the receipt of information about Kaspersky Security Center events from the MS SQL database (hereinafter referred to as MS SQL) in Kaspersky SIEM consists of the following steps:

1 Creating an account in the MS SQL database

To receive Kaspersky Security Center events from MS SQL, a user account is required that has the rights necessary to connect and work with the database.

1. Log in to the server with MS SQL for Kaspersky Security Center installed.
2. Using **SQL Server Management Studio**, connect to MS SQL using an account with administrator rights.
3. In the **Object Explorer** pane, expand the **Security** section.
4. Right-click the **Logins** folder and select **New Login** from the context menu.

   The **Login - New** window opens.
5. On the **General** tab, click the **Search** button next to the **Login name** field.

   The **Select User or Group** window opens.
6. In the **Enter the object name to select (examples)** field, specify the object name and click **OK**.

   The **Select User or Group** window closes.
7. In the **Login - New** window, on the **General** tab, select the **Windows authentication** option.
8. In the **Default database** field, select the Kaspersky Security Center database.

   The default Kaspersky Security Center database name is `KAV`.
9. On the **User Mapping** tab, configure the account permissions:

   a. In the **Users mapped to this login** section, select the Kaspersky Security Center database.

   b. In the **Database role membership for** section, select the check boxes next to the **db_datareader** and **public** permissions.

10. On the **Status** tab, configure the permissions for connecting the account to the database:

    - In the **Permission to connect to database engine** section, select **Grant**.
    - In the **Login** section, select **Enabled**.

11. Click **OK**.

    The **Login - New** window closes.

After creating an account, check the configured rights. To do this, start **SQL Server Management Studio** under the created account, and then go to any MS SQL table and make a selection in this table.

2 Configuring the SQL Server Browser service

After creating an account in MS SQL, you must configure the SQL Server Browser service.

1. Open **SQL Server Configuration Manager**.
2. In the left pane, select **SQL Server Services**.

   A list of services opens.
3. Open the **SQL Server Browser** service properties in one of the following ways:

   - Double-click the name of the **SQL Server Browser** service.
   - Right-click the name of the **SQL Server Browser** service and select **Properties** from the context menu.
4. In the **SQL Server Browser Properties** window that opens, select the **Service** tab.
5. In the **Start Mode** field, select **Automatic**.
6. Select the **Log On** tab and click the **Start** button.

   Automatic startup of the **SQL Server Browser** service is enabled.
7. Enable and configure the **TCP/IP** protocol by doing the following:

   a. In the left pane, expand the **SQL Server Network Configuration** section and select the **Protocols for <SQL Server name>** subsection.

   b. Right-click the **TCP/IP** protocol and select **Enable** from the context menu.

   c. In the **Warning** window that opens, click **OK**.

   d. Open the **TCP/IP** protocol properties in one of the following ways:

      - Double-click the **TCP/IP** protocol.
      - Right-click the **TCP/IP** protocol and select **Properties** from the context menu.

   e. Select the **IP Addresses** tab, and then in the **IPALL** section, specify port 1433 in the **TCP Port** field.

f. Click **Apply** to save the changes.

g. Click **OK** to close the window.

8. Restart the **SQL Server (<SQL Server name>)** service by doing the following:

   a. In the left pane, select **SQL Server Services**.

   b. In the service list on the right, right-click the **SQL Server (<SQL Server name>)** service and select **Restart** from the context menu.

9. In **Windows Defender Firewall with Advanced Security**, allow inbound connections on the server on the TCP port 1433.

3 Creating a secret

After creating and configuring an account in MS SQL, you need to add a secret in the Kaspersky SIEM web interface. This resource is used to store credentials for connecting to MS SQL.

1. In the web interface, go to **Resources** → **Secrets**.

   The list of available secrets will be displayed.

2. Click the **Add secret** button to create a new secret.

   The secret window is displayed.

3. Enter information about the secret:

   a. In the **Name** field, choose a name for the added secret.

   b. In the **Tenant** drop-down list, select the tenant that will own the created resource.

   c. In the **Type** drop-down list, select **urls**.

   d. In the **URL** field, specify a string of the following form:

   ```
   sqlserver://[<domain>%5C]<username>:<password>@<server>:1433/<database_name>
   ```

   where:

   - `domain` is a domain name.
   - `%5C` is the separator between domain and user. Represents the "\" character in URL format.
   - `username` is the name of the created MS SQL account.
   - `password` is the password of the created MS SQL account.

- `server` is the name or IP address of the server where the MS SQL database for Kaspersky Security Center is installed.
- `database_name` is the name of the Kaspersky Security Center database. The default name is KAV.

Example

```
sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV
```

If the MS SQL account password contains special characters (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), convert them to URL format.

4. Click **Save**.

For security reasons, the string specified in the **URL** field is hidden after the secret is saved.

4 Configuring a connector

To connect Kaspersky SIEM to an MS SQL, you need to configure the connector.

1. In the web interface, go to the **Resources** → **Connectors** section.
2. In the list of connectors, find the **[OOTB] KSC SQL** connector and open it for editing.

   If a connector is not available for editing, copy it and open the connector copy for editing. If the **[OOTB] KSC SQL** connector is not available, contact your system administrator.

3. In the **Basic settings** tab, in the **URL** drop-down lists, select the secret created for connection to the MS SQL.
4. Click **Save**.

5 Creating a KUMA collector for receiving Kaspersky Security Center events from the MS SQL database

When creating a collector in the Kaspersky SIEM web interface, at the **Transport** step, select the **[OOTB] KSC SQL** connector, and at the **Event parsing** step, select the **[OOTB] KSC from SQL** normalizer.

6 Installing the KUMA collector in the network infrastructure

Once the collector for receiving Kaspersky Security Center events from MS SQL is created and configured, install the KUMA collector on the network infrastructure server where you intend to receive events.

7 Verifying receipt of events from MS SQL by the KUMA collector

To verify whether receipt of events from MS SQL is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Web Traffic Security

You can configure the receipt of events from the Kaspersky Web Traffic Security (KWTS) web traffic analysis and filtering system in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring export of KWTS events to KUMA

Depending on the version of KWTS, you can use one of the following instructions:

For KWTS 6.2

For KWTS 6.1

To configure the export of KWTS events to KUMA:

1. Connect to the KWTS server over SSH as root.
2. Before making changes, create backup copies of the following files:
   - `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template`
   - `/etc/rsyslog.conf`
3. Make sure that the settings in the `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template` configuration file have the following values, and make changes if necessary:

```
"siemSettings":
{
"enabled": true,
"facility": "Local5",
"logLevel": "Info",
"formatting":
{
```

4. Save your changes.

5. To send events via UDP, make the following changes to the `/etc/rsyslog.conf` configuration file:

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local5.* @<<IP address of the KUMA collector>:<port of the collector>>
```

   If you want to send events over TCP, the last line should be as follows:

```
local5.* @@<<IP address of the KUMA collector>:<port of the collector>>
```

6. Save your changes.

7. Restart the rsyslog service with the following command:

```
sudo systemctl restart rsyslog.service
```

8. Go to the KWTS web interface, to the **Settings** → **Syslog** tab and enable the **Log information about traffic profile** option.

9. Click **Save**.

❷ Configuring export of events in CEF format

If you are configuring the receipt of events from KWTS 6.2, follow the instructions in the KWTS 6.2 documentation to enable export of events.

❸ Creating a KUMA collector for receiving KWTS events

To receive KWTS events, while creating a collector select the **[OOTB] KWTS** normalizer at the **Event parsing** step.

❹ Installing a KUMA collector in the network infrastructure for receiving KWTS events

Once you have created and configured the collector to collect Kaspersky Web Traffic Security events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❺ Verifying receipt of KWTS events by the KUMA collector

To verify whether the KWTS event transmission is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Linux Mail Server

To configure the receipt of events from the Kaspersky Linux Mail Server (KLMS) mail traffic analysis and filtering system to Kaspersky SIEM, follow the steps below:

1 Configuring events export from KLMS to KUMA

Depending on the version of KLMS, you can use one of the following instructions:

For KLMS 10 events to KUMA (KLMS 10 documentation is available in Russian only).

For KLMS 8 in KUMA

To configure the export of KLMS events to KUMA:

1. Connect to the KLMS server over SSH and go to the **Technical Support Mode** menu.
2. Use the klms-control utility to download the settings to the `settings.xml` file:

```
sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f /tmp/settings.xml
```

3. Make sure that the settings in the `/tmp/settings.xml` file have the following values; make changes if necessary:

```
<siemSettings>
        <enabled>1</enabled>
        <facility>Local1</facility>
...
</siemSettings>
```

4. Apply settings with the following command:

```
sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f /tmp/settings.xml
```

5. To send events via UDP, make the following changes to the `/etc/rsyslog.conf` configuration file:

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local1.* @<<collector_IP>:<collector_port>>
```

If you want to send events over TCP, the last line should be as follows:

```
local1.* @@<<collector_IP>:<collector_port>>
```

where:

- <collector_IP> is the collector IP address.
- <collector_port> is the collector port.

6. Save your changes.
7. Restart the rsyslog service with the following command:

```
sudo systemctl restart rsyslog.service
```

2 Creating a KUMA collector for receiving KLMS events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] KLMS syslog CEF** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Kaspersky Linux Mail Server events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of KLMS events by the KUMA collector

To verify whether the KLMS event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Secure Mail Gateway

Configuring the event receiving from the Kaspersky Secure Mail Gateway (KSMG) mail traffic analysis and filtering system to the Kaspersky SIEM consists of the following steps:

1 Configuring sending of KSMG events to Kaspersky SIEM

KSMG can publish events that occur during application operation to Kaspersky SIEM via the Syslog protocol.

Information about each application event is transferred as a separate syslog message in the CEF format. By default, the export of CEF messages is disabled in the application. You can configure the publication of events in the SIEM system and enable the export of events.

2 Creating a KUMA collector for receiving KSMG events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] KSMG** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Kaspersky Secure Mail Gateway events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of KSMG events by the KUMA collector

To verify whether the KSMG event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Industrial CyberSecurity for Networks

Configuring the receiving of events from Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) version 4.2 in Kaspersky SIEM consists of the following steps:

1 Creating a KICS for Networks connector for sending events to KUMA

1. Log in to the KICS for Networks web interface using an administrator account.
2. Go to the **Settings** → **Connectors** section.
3. Click the **Add connector** button.
4. Specify the following settings:
   a. In the **Connector type** drop-down list, select **SIEM**.
   b. In the **Connector name** field, specify a name for the connector.
   c. In the **Server address** field, enter the IP address of the KICS for Networks Server.
   d. In the **Connector deployment node** drop-down list, select the node on which you are installing the connector.
      You can specify any name.
   e. In the **User name** field, specify the user name for Kaspersky SIEM to use for connecting to the application through the connector. You must specify the name of one of the KICS for Networks users.

f. In the **SIEM server address** field, enter the IP address of the KUMA collector server.

g. In the **Port number** field, enter the port number of the KUMA collector.

h. In the **Transport protocol** drop-down list, select **TCP** or **UDP**.

i. Select the **Allow sending audit entries** check box.

j. Select the **Allow sending application entries** check box.

5. Click the **Save** button.

The connector is created. It is displayed in the table of KICS for Networks connectors with the **Running** status.

❷ Configuring export of KICS for Networks events to KUMA

To ensure the sending of KICS for Networks security events to Kaspersky SIEM:

1. Log in to the KICS for Networks web interface using an administrator account.
2. Go to the **Settings** → **Event types** section.
3. Select the check boxes for the types of events that you want to send to Kaspersky SIEM.
4. Click **Select connectors**.
5. In the window that opens, select the connector that you created for sending events to Kaspersky SIEM.
6. Click **OK**.

Events of selected types will be sent to Kaspersky SIEM. In the **Event types** table, such events are marked with a check box in the column with the connector name.

❸ Creating a KUMA collector to receive KICS for Networks events

When creating a collector in the Kaspersky SIEM web interface, you must meet the following requirements:

1. At the **Transport** step, select the type of transport protocol and port number that correspond to those selected when creating the connector in KICS for Networks.
2. At the **Event parsing** step, select the **[OOTB] KICS4Net v3.x** normalizer.
3. At the **Routing** step, make sure that the following destinations are added to the collector resource set:
   - **storage**—used to transmit data to the storage.
   - **correlator**—used to transmit data to the correlator.

If destinations have not been added to the collector, you must create them.

4. At the last step of the wizard, a command is displayed in the lower part of the window, which you can use to install the service on the server that you want to receive events. Copy this command and use it when installing the second part of the collector.

4 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect KICS for Networks events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

5 Verifying receipt of KICS for Networks events by the KUMA collector

To verify whether receipt of events from KICS for Networks is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Anti Targeted Attack Platform

To configure reception of events from Kaspersky Anti Targeted Attack Platform by the Kaspersky SIEM, follow the steps below:

1 Configuring the transfer of Kaspersky Anti Targeted Attack Platform events

1. In a browser on any computer with access to the Central Node server, enter the IP address of the server hosting the Central Node component.

   A window for entering Kaspersky Anti Targeted Attack Platform user credentials opens.

2. In the user credentials entry window, select the **Local administrator** check box and enter the Administrator credentials.

3. Go to the **Settings** → **SIEM system** section.

4. Specify the following settings:

   a. Select the **Activity log** and **Detections** check boxes.

   b. In the **Host/IP** field, enter the IP address or host name of the KUMA collector.

   c. In the **Port** field, specify the port number to connect to the KUMA collector.

   d. In the **Protocol** field, select **TCP** or **UDP** from the list.

   e. In the **Host ID** field, specify the server host ID to be indicated in the SIEM systems log as a detection source.

f. In the **Alert frequency** field, enter the interval for sending messages: from 1 to 59 minutes.

g. If necessary, enable TLS encryption.

5. Click **Apply**.

Export of Kaspersky Anti Targeted Attack Platform events to Kaspersky SIEM is configured.

❷ Creating a KUMA collector for receiving Kaspersky Anti Targeted Attack Platform events

When creating a collector in the Kaspersky SIEM web interface, make sure that the port number and connector type match the port and connector specified in the Kaspersky Anti Targeted Attack Platform event export settings in Kaspersky SIEM. To receive Kaspersky Anti Targeted Attack Platform events using Syslog, select the **[OOTB] KATA** normalizer at the **Event parsing**.

❸ Installing the KUMA collector in the network infrastructure

After creating and configuring the collector for reception of Kaspersky Anti Targeted Attack Platform events, install the KUMA collector on the server of the network infrastructure intended for reception of events.

❹ Verifying receipt of Kaspersky Anti Targeted Attack Platform events by the KUMA collector

To verify whether the Kaspersky Anti Targeted Attack Platform event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface. Kaspersky Anti Targeted Attack Platform events are displayed as KATA in the table with search results.

Kaspersky Endpoint Security for Windows

In Kaspersky Endpoint Security for Windows, starting from version 12.6, events can be sent from Windows logs to a KUMA collector. In this way, KUMA can get events from Windows logs from all hosts with Kaspersky Endpoint Security for Windows 12.6 or later without installing KUMA agents on such hosts.

> Kaspersky Endpoint Security for Windows versions 12.6–12.10 supports a limited set of EventIDs from Microsoft products.
> In Kaspersky Endpoint Security for Windows versions 12.6–12.12, events with similar parameters are filtered and the first of such events is sent, while subsequent similar events are not sent. If a massive amount of similar events occurs, some of them may be sent; hundreds or thousands of similar events are necessary for this to happen. However, a distinct event, such as a different user logging in, is sent. The filtering logic is defined by Kaspersky experts and allows reducing the volume of transmitted events without losing data that is useful for detecting attacks.

To activate this functionality, you need:

- valid Kaspersky SIEM license
- Kaspersky Security Center 14.2 or later
- Kaspersky Endpoint Security for Windows 12.6 or later

Configuring event receiving consists of the following steps:

1 Importing the normalizer into KUMA

In KUMA, you must configure getting updates through Kaspersky update servers.

In the **Resources** section, click **Import resources** and in the list of normalizers available for installation, select **[OOTB] Microsoft Products via KES WIN**.

2 Creating a KUMA collector for receiving Windows events

You have to create a collector to receive Windows events. Depending on the version of Kaspersky Endpoint Security for Windows:

- If you are using Kaspersky Endpoint Security for Windows version 12.6–12.10, at the **Transport** step, select **TCP** or **UDP** and specify the port number that the connector will listen on. At the **Event parsing** step, select the **[OOTB] Microsoft Products via KES WIN** normalizer, and at the **Event filtering** step, select the **[OOTB] Microsoft Products via KES WIN - Event filter for collector** filter.
- If you are using Kaspersky Endpoint Security for Windows version 12.11 or later, at the **Transport** step, select **TCP** or **UDP** and specify the port number that the connector will listen on. At the **Event parsing** step, select one of the following normalizers:
  - For KUMA version 3.2–4.0, select the **[OOTB] Microsoft Products via KES WIN NG for KUMA 3.2** normalizer.
  - For KUMA version 4.0.1 or later, select the **[OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1** normalizer.

3 Requesting a key from Technical Support

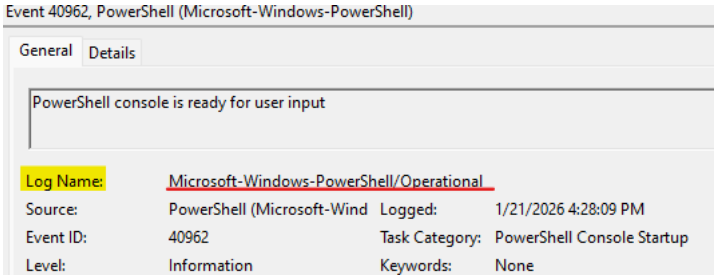
If your license did not include a key for activating the functionality of sending Windows logs to the KUMA collector, send the following message to Technical Support: "We have purchased a KUMA license and are using Kaspersky Endpoint Security for Windows version 12.6. We want to activate the functionality of sending Windows logs to the KUMA collector. Please provide a key file to activate the functionality." New Kaspersky SIEM users do not need to make a Technical Support request because they get two license keys: one for Kaspersky SIEM and one for activating the Kaspersky Endpoint Security for Windows functionality.

In response to your message, you will get a key file.

4 Configuration on the side of Kaspersky Security Center and Kaspersky Endpoint Security for Windows.

A key file that activates the functionality of sending Windows events to KUMA collectors must be imported into Kaspersky Security Center and distributed to Kaspersky Endpoint Security endpoints in accordance with the instructions. You must also add KUMA server addresses to the Kaspersky Endpoint Security policy and specify network connection settings.

> For Kaspersky Endpoint Security for Windows version 12.11 and later, when adding custom logs to the Kaspersky Endpoint Security policy, you need to specify the name of the log to match the value of the **Log name** field in the events of this log (for example, for the Sysmon log, specify Microsoft-Windows-Sysmon/Operational).



The **Log Name** field in a custom Windows log event

5 Verifying receipt of Windows events by the KUMA collector

To verify whether the Windows event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

The list of events from Microsoft products that Kaspersky Endpoint Security for Windows version 12.6–12.10 sends to KUMA is given in the following table.

Event log	Event identifier
System	12 13 7040 7045 42 104 107 109 1074 6005 6006 7034 7036 8003

Event log	Event identifier
Security	1102 4614 4649 4696 4698 4704 4706 4713 4715 4717 4720 4723 4724 4725 4726 4727 4728 4729 4738 4739 4740 4741 4742 4756 4757 4765 4766 4767 4768 4769 4770 4771 4775 4776 4778 4780 4781 4794 4817 4876 4877 4882 4885 4886 4887 4890 4891 4898 4904 4905 4928 4950 4964 5136 5137 5138 5139 5141 5142 5143 5144 5155 5376 5377 5632 5888 5890 6416 4622 4648 4672 4697 4702 4719 4732 4733

Event log	Event identifier
	4798 4946 4947 4948 4949 5145 4616 4625 4663 4624 4799 5140 1008 1105 2722 4615 4618 4626 4627 4634 4647 4653 4654 4656 4657 4658 4659 4660 4661 4664 4666 4667 4670 4673 4674 4688 4689 4690 4691 4692 4693 4694 4695 4699 4700 4701 4703 4705 4707 4714 4716 4718 4730 4731 4734 4737 4743 4744 4745 4746 4747 4748 4749 4750 4751 4752 4753 4754 4755 4758 4759 4760 4761 4762 4763 4764

Event log	Event identifier
	4772 4773 4774 4777 4779 4782 4783 4784 4785 4786 4787 4788 4789 4790 4791 4792 4793 4797 4800 4801 4802 4803 4818 4819 4820 4821 4822 4823 4824 4825 4826 4865 4866 4867 4868 4869 4870 4871 4872 4873 4874 4875 4883 4884 4888 4892 4893 4896 4906 4907 4908 4911 4912 4913 4929 4930 4931 4932 4933 4935 4944 4945 4951 4953 4956 4957 4958 4981 4982 4983 4984 4985 5024 5031 5033 5039

Event log	Event identifier
	5049 5051 5056 5057 5058 5059 5060 5061 5063 5064 5065 5066 5067 5068 5069 5070 5071 5122 5123 5146 5147 5152 5153 5154 5156 5157 5158 5159 5168 5378 5379 5380 5381 5382 5447 5448 5451 5452 5459 5461 5472 5474 5477 5478 5483 5484 5633 6144 6145 6272 6273 6274 6276 6278 6279 6280 6281 6410 6419 6420 6421 6422 6423 6424 6889

Event log	Event identifier
PowerShell	4100 4103 4104 4105 4106 8193 8194 8197 24577 24595 24596 24597 24598 24599 53249 53250 53504
MS SQL Server	615 919 958 1945 2007 2812 3406 3407 3421 3454 5084 5579 5701 5703 6253 8128 9013 9666 15268 15457 17104 17110 17111 17125 17137 17152 17164 17176 17177 17199 17201 17550 17551 17561 17663 18264 18265 18456 18488 18496 19030 19031 19032 26022 26037 26048 26067 33090 49903 49904

Event log	Event identifier
Microsoft Defender	1006 1015 1116 1117 1000 1001 2000 5000 5001 5002 5004 5007 5010 5012
Terminal Server	1149 21 22 24 25 39 40
Microsoft Active Directory Federation Service (AD FS)	106 217 251 335 342 349 358 364 381 385 400 401 417 424 435 436
Sysmon	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 255
Microsoft Active Directory Domain Service (AD DS)	1213 1317 1644 2041 2889

Kaspersky Endpoint Security for Linux

In Kaspersky Endpoint Security for Linux, starting from version 12.2, events can be sent from Linux logs to a KUMA collector. This allows Kaspersky SIEM to receive events from Linux logs from all hosts on which Kaspersky Endpoint Security for Linux version 12.2 is installed. To activate the functionality, you need:

- A valid KUMA license
- Kaspersky Security Center 14.2 or later
- Kaspersky Endpoint Security for Linux 12.2 or later

Configuring event receiving consists of the following steps:

1 Importing the normalizer into KUMA

In Kaspersky SIEM, you must configure updating via the Kaspersky update servers.

In the **Resources** section, click **Resource import** and select **[OOTB] KESL syslog cef** in the list of normalizers available for installation.

2 Creating a KUMA collector for receiving Linux events

When creating a collector in the Kaspersky SIEM web interface, at the **Transport** step, select **TCP** or **UDP** and specify the port number that the collector is listening on. At the **Event parsing** step, select the **[OOTB] KESL syslog cef** normalizer.

3 Requesting a key from Technical Support

If your license did not include a key for activating the functionality of sending Linux logs to the KUMA collector, send the following message to Technical Support: "We have purchased a KUMA license and are using Kaspersky Endpoint Security for Linux version 12.2. We want to activate the functionality of sending Linux logs to the KUMA collector. Please provide a key file to activate the functionality." New Kaspersky SIEM users do not need to make a Technical Support request because they get two license keys: one for Kaspersky SIEM and one for activating the Kaspersky Endpoint Security for Linux functionality.

In response to your message, you will get a key file.

4 Configuring on Kaspersky Security Center and Kaspersky Endpoint Security for Linux side

A key file that activates the functionality of sending Linux events to KUMA collectors must be imported into Kaspersky Security Center and distributed to Kaspersky Endpoint Security endpoints in accordance with the instructions. You must also add KUMA server addresses to the Kaspersky Security Center policy and specify network connection settings.

5 Verifying receipt of Linux events by the KUMA collector

To verify whether the Linux event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Kaspersky Endpoint Security for Linux sends the following events:

- ProcessCreate
- ProcessTerminate
- FileChange
- New user account created
- User account deleted
- Group created
- Group deleted
- New member added to a group
- Member removed from the group
- User password changed
- Linux authentication performed
- Linux session started
- Linux session finished
- Service started
- Service stopped
- Promiscuous mode modified
- Audit configuration changed
- Account expiration date changed

Microsoft

This section describes how to configure the receiving of events from Microsoft products, including Windows and Microsoft 365 cloud services.

KUMA Agent (WEC)

To learn more about collecting event data from Windows devices using a WEC KUMA Agent, watch the video below, and then follow the step-by-step instructions.

https://www.youtube.com/watch?v=bfCCmmOVwO8

Configuring the receiving of information about events from Windows devices using the KUMA Agent of the WEC type consists of the following steps:

1 Configuring audit settings for operating Kaspersky SIEM

You can configure event audit on Windows devices for an individual device or for all devices in a domain using one of the following instructions:

Configuring an audit policy on a Windows device

To configure audit policies on a device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the opened window, type `secpol.msc` and click **OK**.

   The **Local security policy** window opens.
3. Select **Security Settings** → **Local policies** → **Audit policy**.
4. In the pane on the right, double-click to open the properties of the policy for which you want to enable an audit of successful and unsuccessful attempts.

5. In the **<Policy name> properties** window, on the **Local security setting** tab, select the **Success** and **Failure** check boxes to track successful and interrupted attempts.

   It is recommended to enable an audit of successful and unsuccessful attempts for the following policies:

   - Audit Logon
   - Audit Policy Change
   - Audit System Events
   - Audit Logon Events
   - Audit Account Management

Configuration of an audit policy on the device is complete.

Configuring an audit using a group policy

To configure an audit using a group policy:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the opened window, type `gpedit.msc` and click **OK**.

   The **Local Group Policy Editor** window opens.
3. Select **Computer configuration** → **Windows configuration** → **Security settings** → **Local policies** → **Audit policy**.
4. In the pane on the right, double-click to open the properties of the policy for which you want to enable an audit of successful and unsuccessful attempts.
5. In the **<Policy name> properties** window, on the **Local security setting** tab, select the **Success** and **Failure** check boxes to track successful and interrupted attempts.

   It is recommended to enable an audit of successful and unsuccessful attempts for the following policies:

   - Audit Logon
   - Audit Policy Change
   - Audit System Events
   - Audit Logon Events
   - Audit Account Management

> If you want to receive Windows logs from a large number of servers or if installation of KUMA agents on domain controllers is not allowed, it is recommended to configure Windows log redirection to individual servers that have the Windows Event Collector service configured.

The audit policy is now configured on the server or workstation.

❷ Configuring centralized receipt of events using the Windows Event Collector service

The Windows Event Collector service allows you to centrally receive data about events on servers and workstations running Windows. You can use the Windows Event Collector service to subscribe to events that are registered on remote devices.

You can configure the following types of event subscriptions:

- **Source-initiated subscriptions**. Remote devices send event data to the Windows Event Collector server whose address is specified in the group policy.

  Configuring data transfer from the event source server

  You can receive information about events on servers and workstations by configuring data transfer from remote devices to the Windows Event Collector server.

  Preliminary steps

  1. Verify that the Windows Remote Management service is configured on the event source server by running the following command in the PowerShell console:

     ```
     winrm get winrm/config
     ```

     If the Windows Remote Management service is not configured, initialize it by running the following command:

     ```
     winrm quickconfig
     ```

  2. If the event source server is a domain controller, make the Windows logs available over the network by running the following command in PowerShell as an administrator:

     ```
     wevtutil set-log security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)'
     ```

     Verify access by running the following command:

     ```
     wevtutil get-log security
     ```

  Configuring the firewall on the event source server

  To enable the Windows Event Collector server to receive Windows log entries, inbound connection ports must be opened on the event source server.

  To open ports for inbound connections:

  1. On the event source server, open the **Run** window by pressing the key combination **`Win`**+**`R`**.

  2. In the opened window, type `wf.msc` and click **OK**.

     The **Windows Defender Firewall with Advanced Security** window opens.

  3. Go to the **Inbound Rules** section and click **New Rule** in the **Actions** pane.

     The **New Inbound Rule Wizard** opens.

  4. At the **Rule type** step, select **Port**.

5. At the **Protocols and ports** step, select **TCP** as the protocol. In the **Specific local ports** field, indicate the relevant port numbers:

   - `5985` (for HTTP access)
   - `5986` (for HTTPS access)

   You can indicate one of the ports, or both.

6. At the **Action** step, select **Allow connection** (selected by default).
7. At the **Profile** step, clear the **Private** and **Public** check boxes.
8. At the **Name** step, specify a name for the new inbound connection rule and click **Done**.

Configuration of data transfer from the event source server is complete.

> The Windows Event Collector server must have the permissions to read Windows logs on the event source server. These permissions can be assigned to both the Windows Event Collector server account and to a special user account. For details on granting permissions, please refer to the "Granting user permissions to view the Windows Event Log" section.

- **Collector-initiated subscriptions**. The Windows Event Collector server connects to remote devices and independently gathers events from local logs.

  Configuring the Windows Event Collector service

  The Windows Event Collector server can independently connect to devices and gather data on events of any severity.

  To configure the receipt of event data by the Windows Event Collector server:

  1. On the event source server, open the **Run** window by pressing **`Win`**+**`R`**.
  2. In the opened window, type `services.msc` and click **OK**.

     The **Services** window opens.

  3. In the list of services, find and start the **Windows Event Collector** service.
  4. Open the **Event Viewer** snap-in by doing the following:

     a. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

     b. In the opened window, type `eventvwr` and click **OK**.

  5. Go to the **Subscriptions** section and click **Create Subscription** in the **Actions** pane.
  6. In the opened **Subscription Properties** window, specify the name and description of the subscription, and define the following settings:

     a. In the **Destination log** field, select **ForwardedEvents** from the list.

     b. In the **Subscription type and source computers** section, click the **Select computers** button.

c. In the opened **Computers** window, click the **Add domain computer** button.

The **Select computer** window opens.

d. In the **Enter the object names to select (examples)** field, list the names of the devices from which you want to receive event information. Click **OK**.

e. In the **Computers** window, check the list of devices from which the Windows Event Collector server will gather event data and click **OK**.

f. In the **Subscription properties** window, in the **Collected events** field, click the **Select events** button.

g. In the opened **Request filter** window, specify how often and which data about events on devices you want to receive.

h. If necessary, in the **<All event codes>** field, list the codes of the events whose information you want to receive or do not want to receive. Click **OK**.

7. If you want to use a special account to view event data, do the following:

a. In the **Subscription properties** window, click the **Advanced** button.

b. In the opened **Advanced subscription settings** window, in the user account settings, select **Specific user**.

c. Click the **User and password** button and enter the account credentials of the selected user.

Configuration of the Event Collector Service is complete.

To verify that the configuration is correct and event data is being received by the Windows Event Collector server:

In the **Event Viewer** snap-in, go to **Event Viewer (Local)** → **Windows logs** → **ForwardedEvents**.

❸ Granting permissions to view events

You can grant permissions to view Windows events for a specific device or for all devices in a domain.

Granting permissions to view events on a specific device

To grant permissions to view events on a specific device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

2. In the opened window, type `compmgmt.msc` and click **OK**.

   The **Computer Management** window opens.

3. Go to **Computer Management (local)** → **Local users and groups** → **Groups**.

4. In the pane on the right, select the **Event Log Readers** group and double-click to open the policy properties.

5. Click the **Add** button at the bottom of the **Properties: Event Log Readers** window.

   The **Select Users, Computers or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant permissions to view event data.

7. Click **OK**.

Granting permissions to view events for all devices in a domain

To grant permissions to view events for all devices in a domain:

1. Log in to the domain controller with administrator privileges.

2. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

3. This opens a window; in that window, type `dsa.msc` and click **OK**.

   The **Active Directory Users and Computers** window opens.

4. Go to **Active Directory Users and Computers** → **<Domain name>** → **Builtin**.

5. In the pane on the right, select the **Event Log Readers** group and double-click to open the policy properties.

   In the **Properties: Event Log Readers** window, open the **Members** tab and click the **Add** button.

   The **Select Users, Computers or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant permissions to view event data.

7. Click **OK**.

4 Granting permissions to log on as a service

You can grant permission to log on as a service to a specific device or to all devices in a domain. The "Log on as a service" permission allows you to start a process using an account that has been granted this permission.

Granting login permissions as a service to a specific device

> Before granting the permission, make sure that the accounts or devices to which you want to grant the **Log on as a service** permission are not listed in the properties of the **Deny log on as a service** policy.

To grant the "Log on as a service" permission to a device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

2. In the opened window, type `secpol.msc` and click **OK**.

   The **Local security policy** window opens.

3. Go to **Security settings** → **Local policies** → **User rights assignment**.

4. In the pane on the right, double-click to open the properties of the **Log on as a service** policy.

5. In the opened **Properties: Log on as a Service** window, click the **Add User or Group** button.

   The **Select Users or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the accounts or devices to which you want to grant the permission to log on as a service.

7. Click **OK**.

Grating the "Log on as a service" permission to all devices in a domain

> Before granting the permission, make sure that the accounts or devices to which you want to grant the **Log on as a service** permission are not listed in the properties of the **Deny log on as a service** policy.

To grant the "Log on as a service" permission to devices in a domain:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

2. In the opened window, type `gpedit.msc` and click **OK**.

   The **Local Group Policy Editor** window opens.

3. Select **Computer configuration** → **Windows configuration** → **Security settings** → **Local policies** → **User rights assignment**.

4. In the pane on the right, double-click to open the properties of the **Log on as a service** policy.

5. In the opened **Properties: Log on as a Service** window, click the **Add User or Group** button.

   The **Select Users or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant the permission to log on as a service.

7. Click **OK**.

❺ Creating a KUMA collector for receiving events from Windows devices

Create a collector in the Kaspersky SIEM web interface for events from Windows devices, and specify the following settings:

1. At the **Transport** step, define the following settings:

   a. In the **Connector** window, select **Create**.

   b. In the **Type** field, select **http**.

   c. In the **Delimiter** field, select **\0**.

2. On the **Advanced settings** tab, in the **TLS mode** field, select **Enabled**.

3. At the **Event parsing** step, click the **Add event parsing** button.

4. This opens the **Basic event parsing** window; in that window, in the **Normalizer** field, select **[OOTB] Microsoft Products** and click **OK**.

5. At the **Routing** step, add the following destinations:

   - **Storage**. To send processed events to the storage.
   - **Correlator**. To send processed events to the correlator.

   If the **Storage** and **Correlator** destinations were not added, create them.

6. At the **Setup validation** tab, click **Create and save service**.

7. Copy the command for installing the KUMA collector that appears.

6 Installing the KUMA collector in the network infrastructure

After creating and configuring the collector for reception of events from Windows devices, install the KUMA collector on the server of the network infrastructure intended for reception of events.

7 Transferring events from Windows devices to KUMA

To complete the data forwarding configuration, you must create a WEC KUMA agent and then install it on the device from which you want to receive event information.

For more details on creating and installing a WEC KUMA Agent on Windows devices, please refer to the Forwarding events from Windows devices to KUMA section.

KUMA Agent (WMI)

To learn more about collecting event data from Windows devices using a WMI KUMA Agent, watch the video below, and then follow the step-by-step instructions.

https://www.youtube.com/watch?v=bfCCmmOVwO8

Configuring the receiving of information about events from Windows devices using the KUMA Agent of the WMI type consists of the following steps:

1 Configuring audit settings for operating Kaspersky SIEM

You can configure event audit on Windows devices for an individual device or for all devices in a domain using one of the following instructions:

Configuring an audit policy on a particular Windows device

To configure audit policies on a device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the opened window, type `secpol.msc` and click **OK**.

   The **Local security policy** window opens.
3. Select **Security Settings** → **Local policies** → **Audit policy**.
4. In the pane on the right, double-click to open the properties of the policy for which you want to enable an audit of successful and unsuccessful attempts.
5. In the **<Policy name> properties** window, on the **Local security setting** tab, select the **Success** and **Failure** check boxes to track successful and interrupted attempts.

   It is recommended to enable an audit of successful and unsuccessful attempts for the following policies:

   - Audit Logon
   - Audit Policy Change
   - Audit System Events
   - Audit Logon Events
   - Audit Account Management

Configuration of an audit policy on the device is complete.

Configuring an audit using a group policy

To configure an audit using a group policy:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the opened window, type `gpedit.msc` and click **OK**.

   The **Local Group Policy Editor** window opens.
3. Select **Computer configuration** → **Windows configuration** → **Security settings** → **Local policies** → **Audit policy**.
4. In the pane on the right, double-click to open the properties of the policy for which you want to enable an audit of successful and unsuccessful attempts.
5. In the **<Policy name> properties** window, on the **Local security setting** tab, select the **Success** and **Failure** check boxes to track successful and interrupted attempts.

It is recommended to enable an audit of successful and unsuccessful attempts for the following policies:

- Audit Logon
- Audit Policy Change
- Audit System Events
- Audit Logon Events
- Audit Account Management

> If you want to receive Windows logs from a large number of servers or if installation of KUMA agents on domain controllers is not allowed, it is recommended to configure Windows log redirection to individual servers that have the Windows Event Collector service configured.

The audit policy is now configured on the server or workstation.

2 Preliminary steps before configuring data transfer from an event source server

1. On the event source server, open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the window that opens, enter the query:

   ```
   services.msc
   ```

3. Click **OK**.

   The **Services** window opens.
4. In the list of services, find the following services:
   - **Remote Procedure Call**.
   - **RPC Endpoint Mapper**.
5. Check the **Status** column to confirm that these services have the **Running** status.

3 Configuring the firewall on the event source server

The Windows Management Instrumentation server can receive Windows log entries if ports are open for inbound connections on the event source server.

To open ports for inbound connections:

1. On the event source server, open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the window that opens, enter the query:

   ```
   wf.msc
   ```

3. Click **OK**.
4. In the **Windows Defender Firewall with Advanced Security** window that is displayed, go to the **Inbound Rules** section and in the **Actions** pane, click **New Rule**.

   This opens the **New Inbound Rule Wizard**.
5. At the **Rule type** step, select **Port**.
6. At the **Protocols and ports** step, select **TCP** as the protocol, and in the **Specific local ports** field, specify the relevant port numbers:
   - 135
   - 445
   - 49152–65535
7. At the **Action** step, select **Allow connection** (selected by default).
8. At the **Profile** step, clear the **Private** and **Public** check boxes.
9. At the **Name** step, specify a rule name for the new inbound connection.
10. Click **Finish**.

    Configuration of data transfer from the event source server is complete.

If the ports are closed, the The RPC server is unavailable error is returned.

4 Granting permissions to view events

You can grant permissions to view Windows events for a specific device or for all devices in a domain.

Granting permissions to view events on a specific device

To grant permissions to view events on a specific device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.
2. In the opened window, type `compmgmt.msc` and click **OK**.

   The **Computer Management** window opens.
3. Go to **Computer Management (local)** → **Local users and groups** → **Groups**.

4. In the pane on the right, select the **Event Log Readers** group and double-click to open the policy properties.

5. Click the **Add** button at the bottom of the **Properties: Event Log Readers** window.

   The **Select Users, Computers or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant permissions to view event data.

7. Click **OK**.

Granting permissions to view events for all devices in a domain

To grant permissions to view events for all devices in a domain:

1. Log in to the domain controller with administrator privileges.

2. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

3. This opens a window; in that window, type `dsa.msc` and click **OK**.

   The **Active Directory Users and Computers** window opens.

4. Go to **Active Directory Users and Computers** → **<Domain name>** → **Builtin**.

5. In the pane on the right, select the **Event Log Readers** group and double-click to open the policy properties.

   In the **Properties: Event Log Readers** window, open the **Members** tab and click the **Add** button.

   The **Select Users, Computers or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant permissions to view event data.

7. Click **OK**.

5 Granting permissions to log on as a service

You can grant permission to log on as a service to a specific device or to all devices in a domain. The "Log on as a service" permission allows you to start a process using an account that has been granted this permission.

Granting login permissions as a service to a specific device

> Before granting the permission, make sure that the accounts or devices to which you want to grant the **Log on as a service** permission are not listed in the properties of the **Deny log on as a service** policy.

To grant the "Log on as a service" permission to a device:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

2. In the opened window, type `secpol.msc` and click **OK**.

   The **Local security policy** window opens.

3. Go to **Security settings** → **Local policies** → **User rights assignment**.

4. In the pane on the right, double-click to open the properties of the **Log on as a service** policy.

5. In the opened **Properties: Log on as a Service** window, click the **Add User or Group** button.

   The **Select Users or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the accounts or devices to which you want to grant the permission to log on as a service.

7. Click **OK**.

Grating the "Log on as a service" permission to all devices in a domain

> Before granting the permission, make sure that the accounts or devices to which you want to grant the **Log on as a service** permission are not listed in the properties of the **Deny log on as a service** policy.

To grant the "Log on as a service" permission to devices in a domain:

1. Open the **Run** window by pressing the key combination **`Win`**+**`R`**.

2. In the opened window, type `gpedit.msc` and click **OK**.

   The **Local Group Policy Editor** window opens.

3. Select **Computer configuration** → **Windows configuration** → **Security settings** → **Local policies** → **User rights assignment**.

4. In the pane on the right, double-click to open the properties of the **Log on as a service** policy.

5. In the opened **Properties: Log on as a Service** window, click the **Add User or Group** button.

   The **Select Users or Groups** window opens.

6. In the **Enter the object names to select (examples)** field, list the names of the users or devices to which you want to grant the permission to log on as a service.

7. Click **OK**.

6 Creating a KUMA collector for receiving events from Windows devices

When creating a collector in the Kaspersky SIEM web interface, select **[OOTB] Microsoft Products** in the **Normalizer** field at the **Event parsing** step.

7 Installing the KUMA collector in the network infrastructure

After creating and configuring the collector for reception of events from Windows devices, install the KUMA collector on the server of the network infrastructure intended for reception of events.

8 Transferring events from Windows devices to Kaspersky SIEM

To complete the data forwarding configuration, you must create a WMI KUMA agent and then install it on the device from which you want to receive event information.

For more details on creating and installing a WMI KUMA Agent on Windows devices, please refer to the Transferring events from Windows devices to KUMA section.

Event Tracing for Windows connector

The *Event Tracing for Windows* connector (hereinafter also referred to as the ETW connector) is a mechanism for logging events generated by applications and drivers on the DNS server. You can use the ETW connector to troubleshoot errors during development or to look for malicious activity.

The impact of the ETW connector on DNS server performance is insignificant. For example, a DNS server running on modern hardware and getting up to 100,000 queries per second (QPS) may experience a 5% performance drop while using the ETW connector. If the DNS server gets up to 50,000 requests per second, no performance drop is observed. We recommend monitoring DNS server performance when using the ETW connector, regardless of the number of requests per second.

By default, you can use the ETW connector on Windows Server 2016 or later. The ETW connector is also supported by Windows Server 2012 R2 if the update for event logging and change auditing is installed. The update is available on the Microsoft Support website.

The ETW connector consists of the following components:

- *Providers* are elements of the system that generate events and send them to the ETW connector. For example, Windows kernels or device drivers can act as providers. When working with code, developers must specify which events the providers must send to the ETW connector. An event may represent the execution of a function that the developer considers important, for example, a function that allows access to the Security Account Manager (SAM).

- *Consumers* are software systems that receive events generated by providers from the ETW connector, and use these events in some way. For example, KUMA can act as a consumer.

- *Controllers* are pieces of software that manage the interaction between providers and consumers. For example, the Logman or Wevtutil utilities can be controllers. Providers register with the controller to send events to consumers. The controller can enable or disable a provider. If a provider is disabled, it does not generate events.

Controllers use trace sessions for communication between providers and consumers. Trace sessions are also used for filtering data based on specified parameters because consumers may need different events.

Configuring DNS server event reception using the ETW connector involves the following steps:

1 Configuration on the Windows side

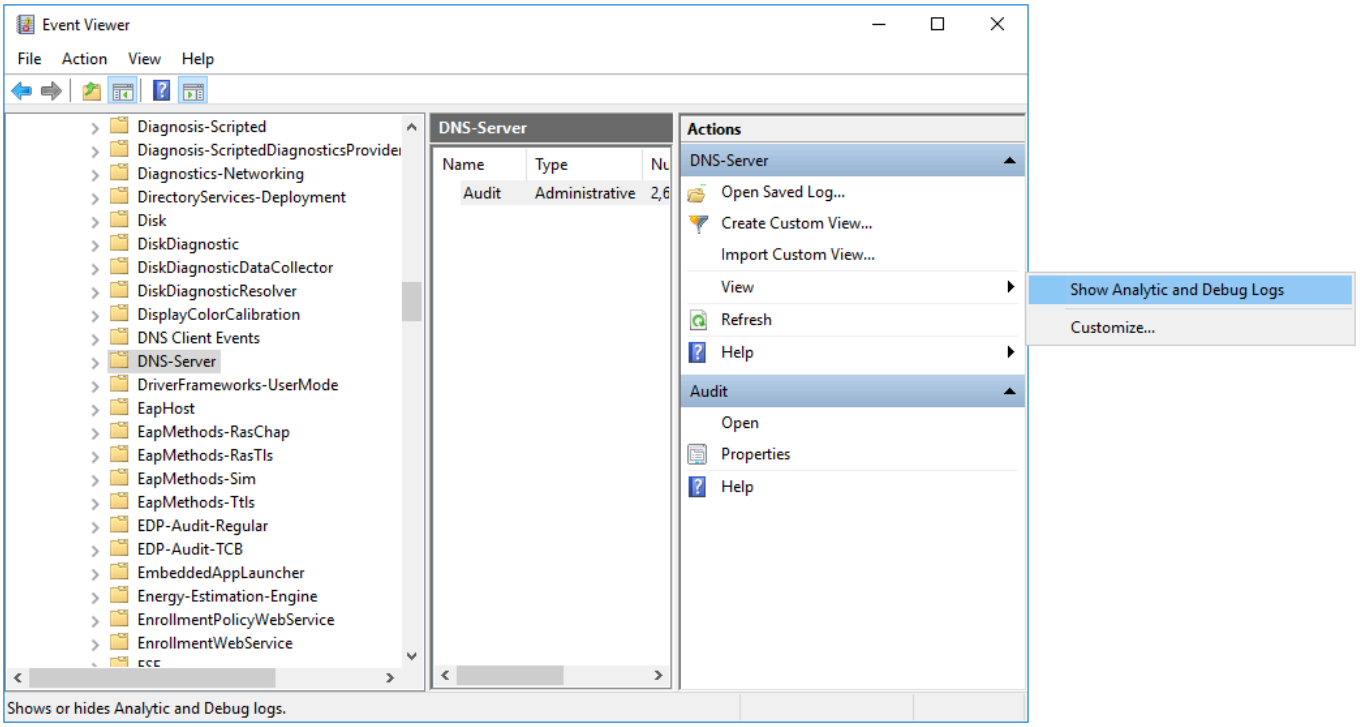
To configure the reception of DNS server events using the ETW connector on the Windows side:

1. Start the Event viewer by running the following command:

```
eventvwr.msc
```

2. This opens a window; in that window, go to the **Applications and Services Logs** → **Microsoft** → **Windows** → **DNS-Server** folder.

3. Open the context menu of the **DNS-Server** folder and select **View** → **Show Analytic and Debug Logs**.

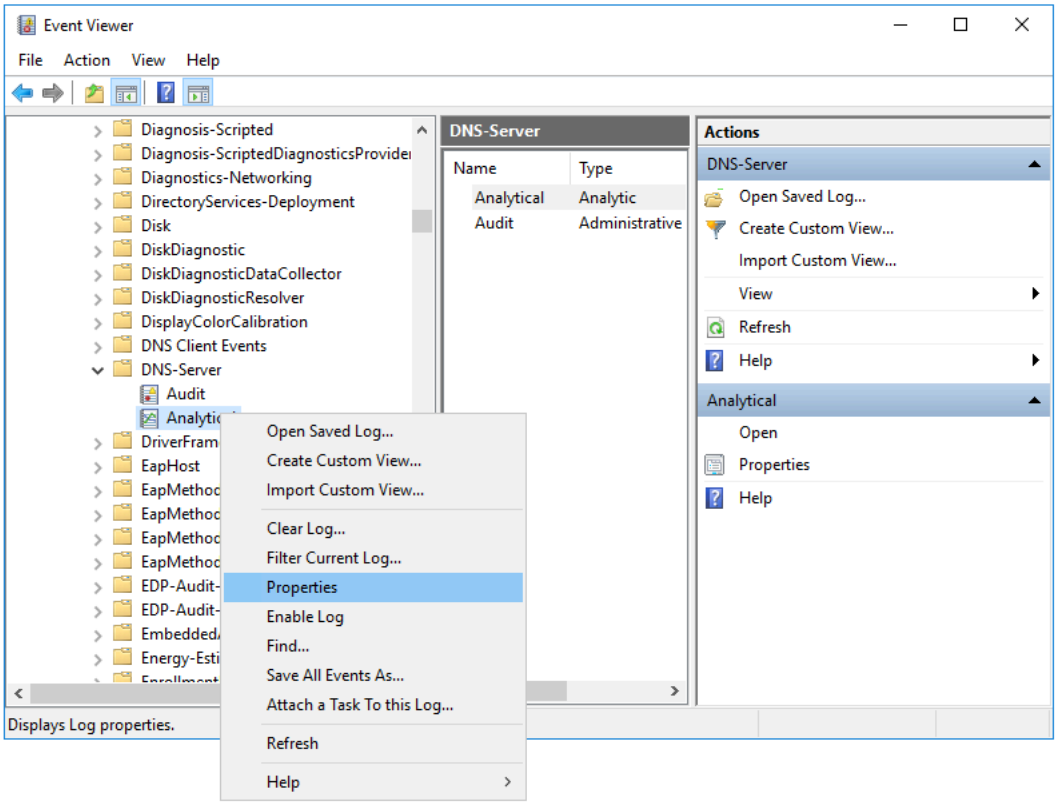


Displaying the analytical and debug logs

The **Audit** debug log and **Analytical** log are displayed.

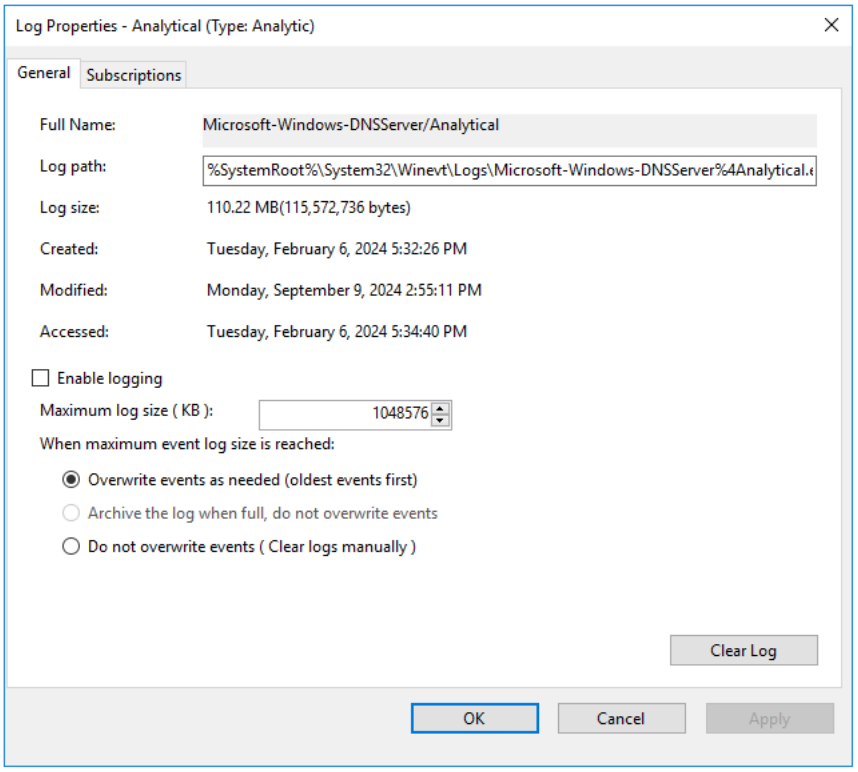
4. Configure the analytic log:

a. Open the context menu of the **Analytical** log and select **Properties**.



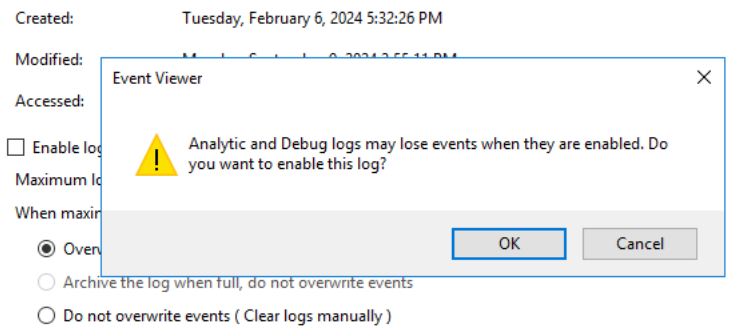
Go to the properties of the Analytical log

a. This opens a window; in that window, make sure that in the **Max Log Size (KB)** field, the value is `1048576`.



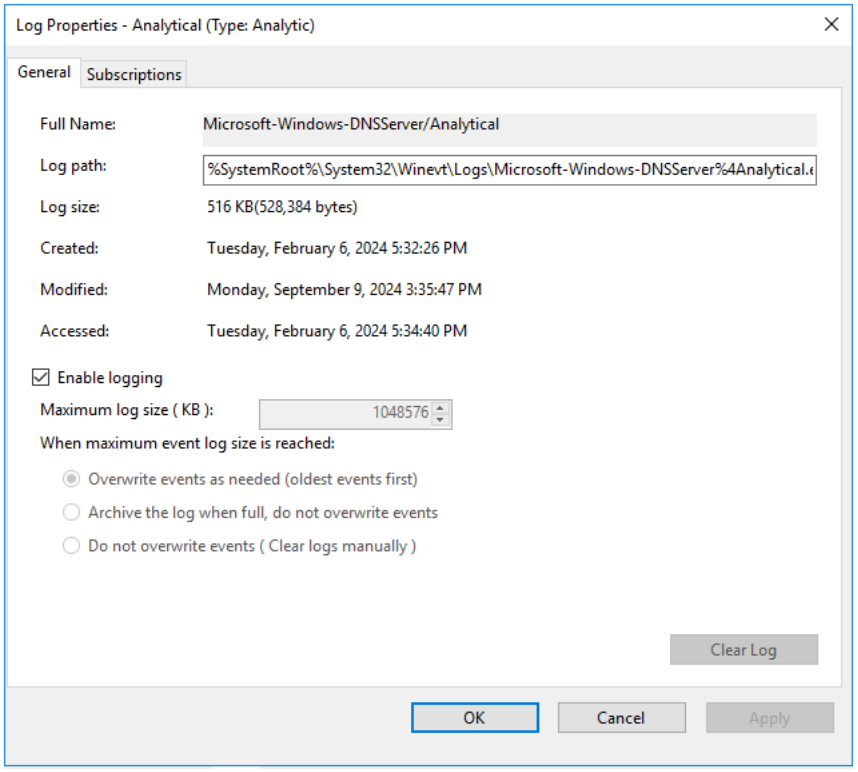
Analytical log properties

a. Select the **Enable logging** check box and in the confirmation window, click **OK**.



Confirmation window

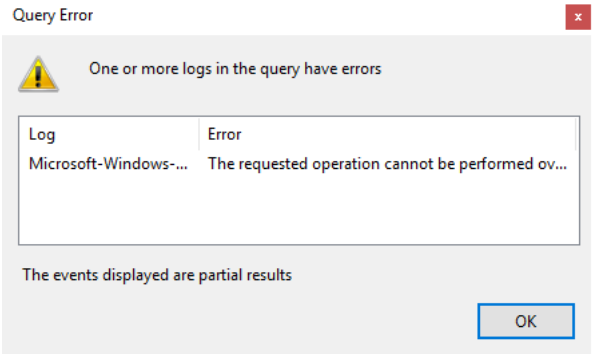
The analytic log must be configured as follows:



Reviewing the settings of the Analytical log for correctness

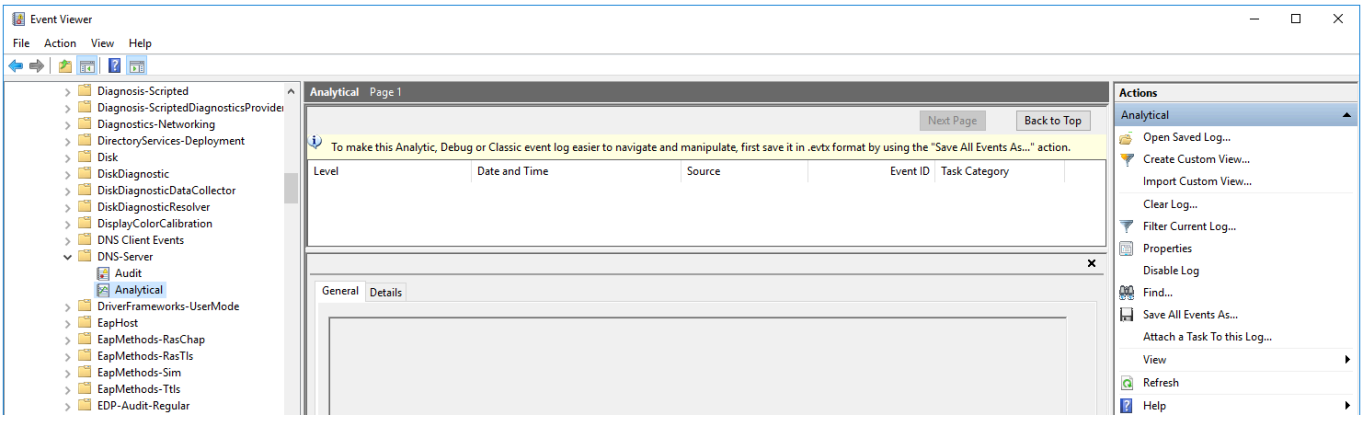
a. Click **Apply**, then click **OK**.

   An error notification is displayed.



Error window

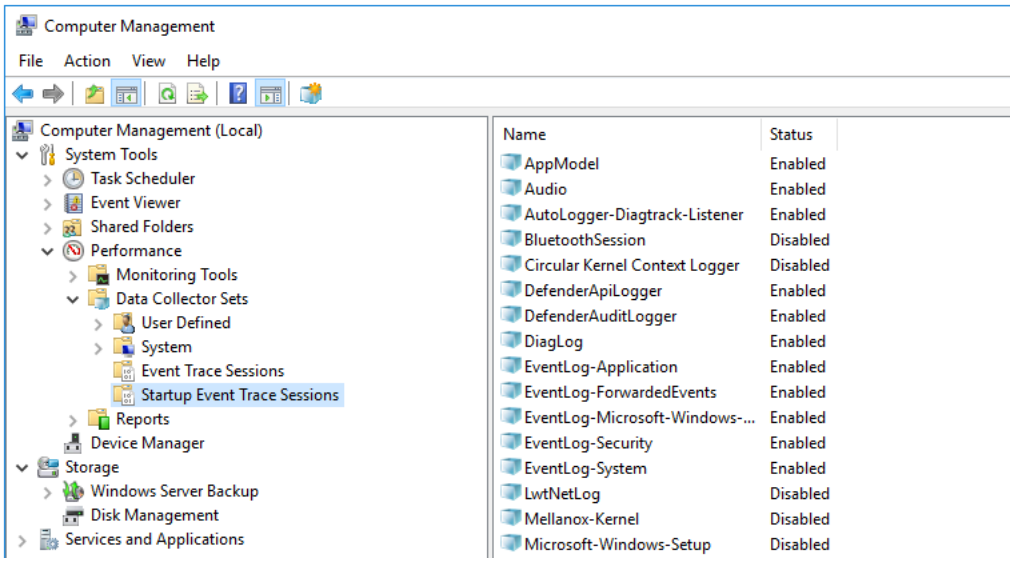
When analytic log rotation is enabled, events are not displayed. To view events, in the **Actions** pane, click **Stop logging**.



Stopping logging

5. Start Computer management as administrator.

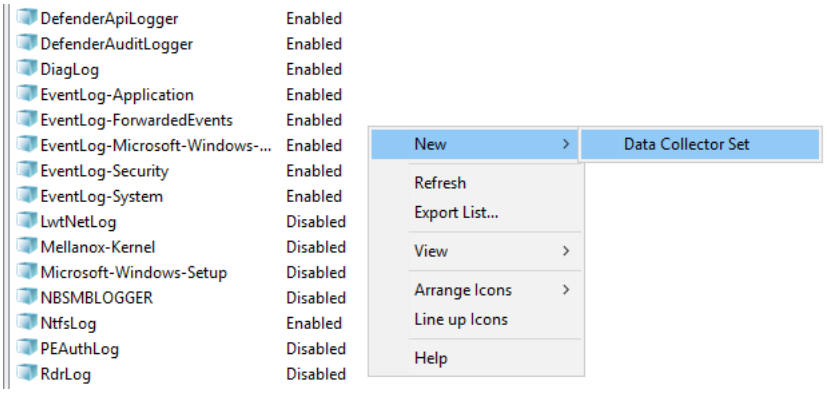
6. This opens a window; in that window, go to the **System Tools** → **Performance** → **Startup Event Trace Sessions** folder.



Managing the computer

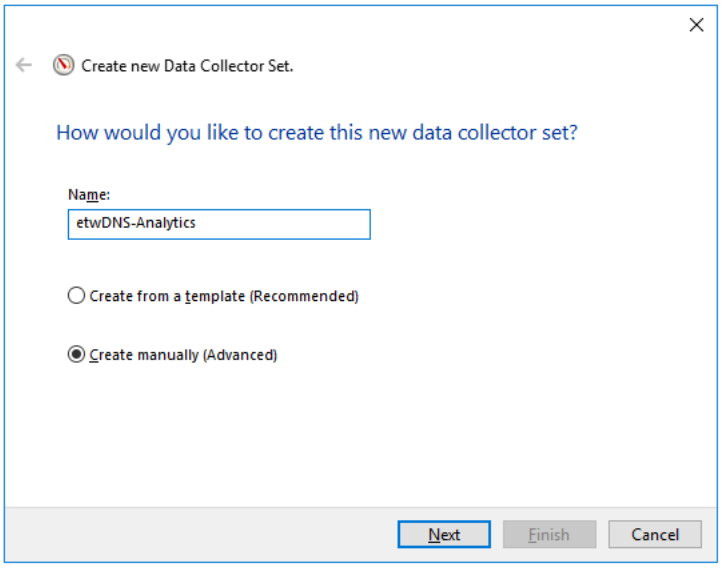
7. Create a provider:

a. Open the context menu of the **Startup Event Trace Sessions** folder and select **Create** → **Data Collector Set**.



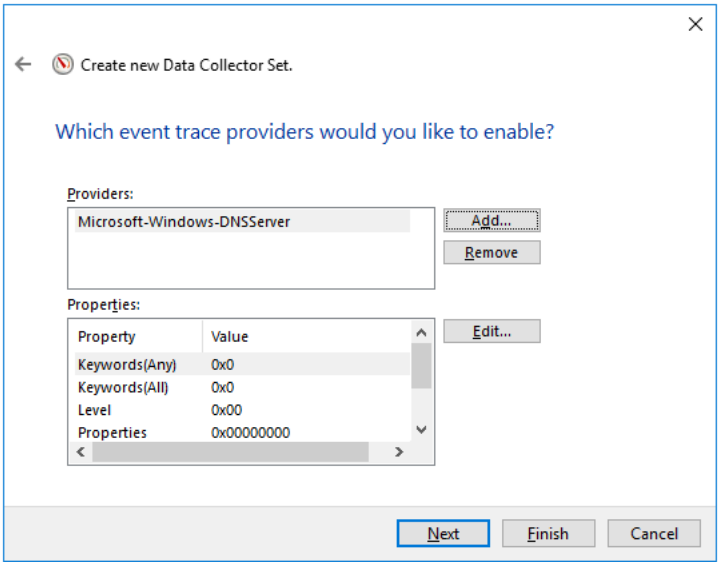
Creating a data collector group

a. This opens a window; in that window, enter the name of the provider and click **Next**.



Entering the provider name

a. Click **Add...** and in the displayed window, select the **Microsoft-Windows-DNSServer** provider.

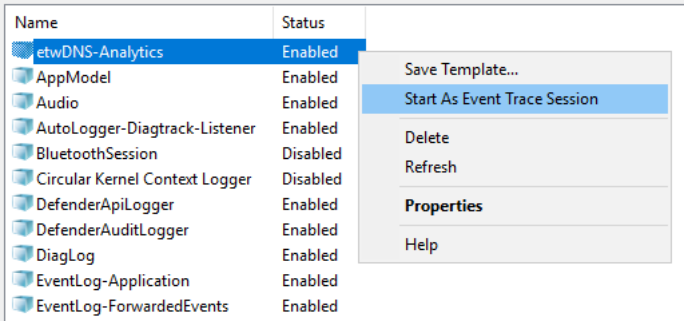


Selecting a provider

The KUMA agent with the ETW connector works only with System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer.

a. Click **Next** twice, then click **Finish**.

8. Open the context menu of the created provider and select **Start As Event Trace Session**.



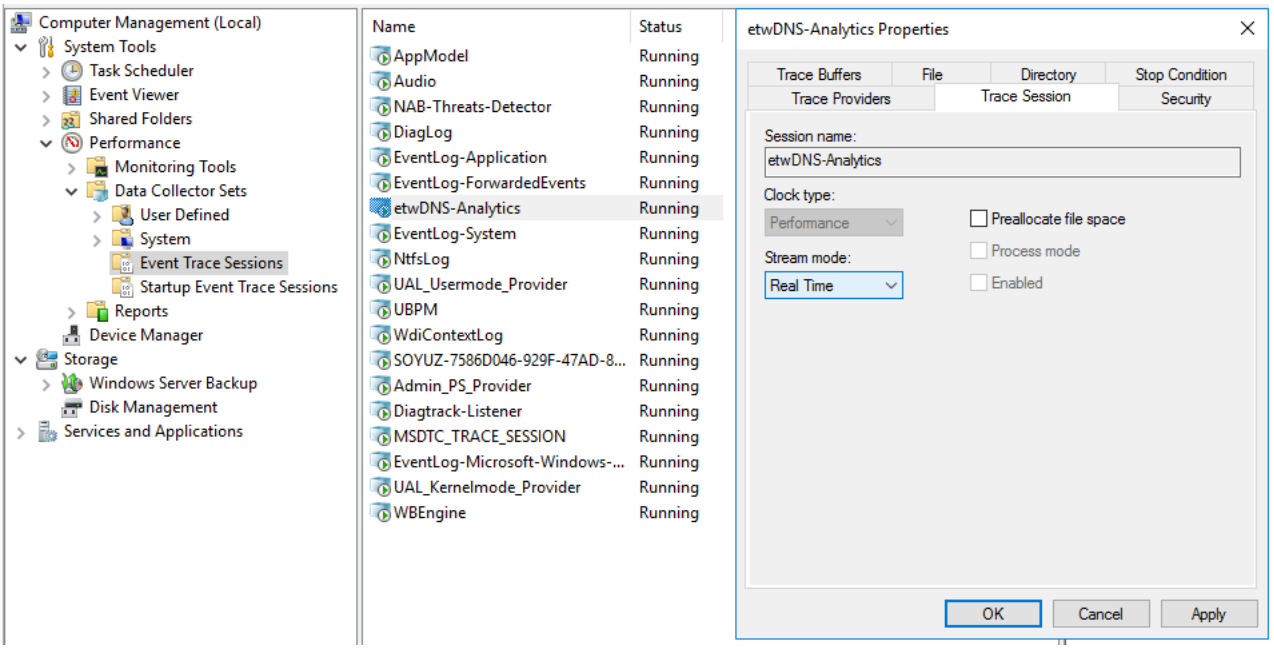
Starting the provider

9. Go to the **Event Trace Sessions** folder.

   Event trace sessions are displayed.

10. Open the context menu of the created event trace session and select **Properties**.

11. This opens a window; in that window, select the **Trace Sessions** tab and in the **Stream Mode** drop-down list, select **Real Time**.



Configuring stream mode

12. Click **Apply**, then click **OK**.

DNS server event reception using the ETW connector is configured.

2 Creating a KUMA collector to receive DNS server events using the ETW connector

When creating a KUMA collector, follow these steps:

1. At step 2 of the Collector Installation Wizard perform the following actions:

   a. In the **Type** drop-down list, select the **tcp** or **http** connector type.

   b. In the **URL** field, enter the FQDN and port number on which the KUMA collector will listen for a connection from the KUMA agent. You can specify any unoccupied port number.

   c. In the **Delimiter** field, enter `\n`.

2. At step 3 of the Collector Installation Wizard, in the **Normalizer** drop-down list, select a normalizer. We recommend selecting the predefined extended normalizer for Windows events, **[OOTB] Microsoft DNS ETW logs json**.

3. At step 7 of the Collector Installation Wizard, add a **Storage** type destination for storing events. If you plan to use event correlation, you also need to add a **Correlator** type destination.

4. At step 8 of the Collector Installation Wizard, click **Create and save service**, and in the lower part of the window, copy the command for installing the KUMA collector on the server.

3 Installing the KUMA collector in the network infrastructure

1. Connect to the KUMA command line interface using a user account with root privileges.

2. Install the KUMA collector by running the command that you copied at step 8 of the Collector Installation Wizard.

3. If you want to add the KUMA collector port to the firewall exclusions and update the firewall settings, run the following commands:

```
firewall-cmd --add-port=<collector port number>/tcp --permanent
firewall-cmd --reload
```

The KUMA collector is installed and the status of the KUMA collector service changes to green in the Kaspersky SIEM web interface.

4 Creating a KUMA agent

When creating a KUMA agent, follow these steps:

1. Go to the **Connection 1** tab.
2. Under **Connector**, in the **Connector** drop-down list, select **Create** and specify the following settings:
   a. In the **Type** drop-down list, select the **etw** connector type.
   b. In the **Session name** field, enter the provider name that you specified when you configured the reception of DNS server events using the ETW connector on the Windows side.
3. Under **Destinations**, in the **Destination** drop-down list, select **Create** and specify the following settings:
   a. In the **Type** drop-down list, select the **tcp** destination type.
   b. In the **URL** field, enter the FQDN and port number on which the KUMA collector will listen for a connection from the KUMA agent. The value must match the value that you specified at step 2 of the Collector Installation Wizard.
4. Go to the **Advanced settings** tab, and in the **Disk buffer size limit** field, enter:

```
1073741824
```

5 Creating a KUMA agent service

Copy the ID of the created KUMA agent service in the **Resources** → **Active services** section. To do so, right-click next to the KUMA agent service and select **Copy ID** in the context menu.

6 Creating an account for the KUMA agent

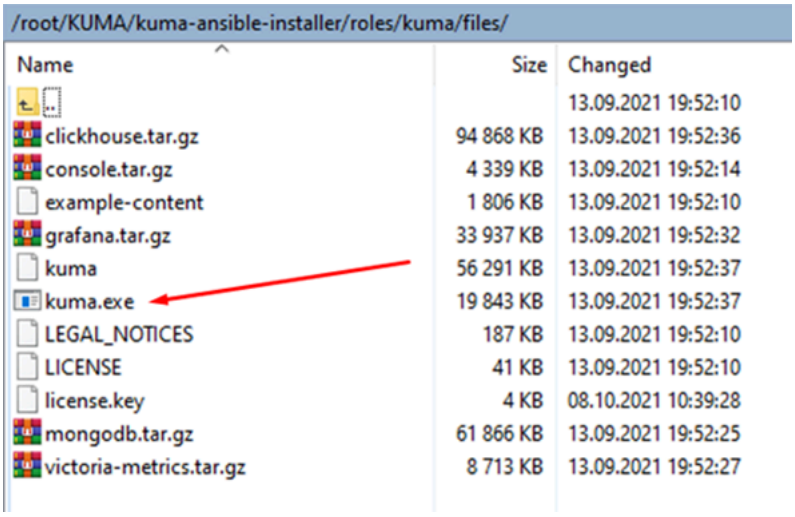
Create a domain or local Windows user account for running the KUMA agent and reading the analytic log. You need to add the created user account to the **Performance Log Users** group and grant the **Log on service** permission (**Log on as a service**).

7 Installing a KUMA agent on a Windows server

You need to install the KUMA agent on the Windows server that will be receiving events from the provider. To do so:

1. Add the FQDN of the KUMA Core server to the `hosts` file on the Windows server or to the DNS server.
2. Create the `C:\Users\<user name>\Desktop\KUMA` folder on the Windows server.

3. Copy the `kuma.exe` file from the KUMA installation package archive to the `C:\Users\<user name>\Desktop\KUMA` folder.



4. Run the command interpreter as administrator.

5. Go to the `C:\Users\<user name>\Desktop\KUMA` folder and run the following command:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id <KUMA agent service ID>
```

In the Kaspersky SIEM web interface, in the **Resources** → **Active services** section, make sure that the KUMA agent service is running and its status is now green, and then abort the command.

6. Start the KUMA Agent installation in one of the following ways:

- If you want to start the KUMA agent installation using a domain user account, run the following command:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <KUMA agent service ID> --user <domain>\<user account name for the KUMA agent> --install
```

- If you want to start the agent installation using a local user account, run the following command:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <KUMA agent service ID> --user <user account name for the KUMA agent> --install
```

where:

`<fingerprint ID of the KUMA Core CA certificate>` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

You will need to enter the password of the KUMA agent user account.

The KUMA Windows Agent service <KUMA agent service ID> is installed on the Windows server. In the Kaspersky SIEM web interface, in the **Resources** → **Active services** section, if the KUMA agent service is not running and has the red status, you need to make sure that port 7210 is available, as well as the Windows collector port in the direction from the KUMA agent to the KUMA collector.

To remove the KUMA agent service on the Windows server, run the following command:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --id <KUMA agent service ID> --uninstall
```

8 Verifying receipt of DNS server events by the KUMA collector

To verify whether ETW connector is configured to receive DNS server events, you can search for related events in the Kaspersky SIEM web interface.

Microsoft 365

You can configure the receipt of events from the Microsoft 365 (Office 365) cloud solution in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring access to Office 365 management APIs https://learn.microsoft.com/en-us/office/office-365-management-api/get-started-with-office-365-management-apis using standard Microsoft methods

To receive events in Kaspersky SIEM, grant the necessary set of API permissions:

- **Microsoft.Graph**
- **Directory.Read.All**
- **Office 365 management API**
- **ActivityFeed.Read**
- **ActivityFeed.Read.Dlp**

2 Creating a KUMA collector for receiving Microsoft 365 events

When creating a collector in the Kaspersky SIEM web interface, at the **Transport** step, specify the **office365** connector type, and at the **Event parsing** step, specify the **[OOTB] Microsoft Office 365 json** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Microsoft 365 events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Microsoft 365 events by the KUMA collector

To verify whether the Microsoft 365 event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Unix and Linux

This section describes how to configure the receiving of events from Linux and Unix servers and systems, including auditing, authentication services, and web servers.

Auditd

Configuring the reception of Auditd events on Linux devices involves the following steps:

1 Creating a KUMA collector for receiving Auditd events

To receive Auditd events when creating a collector, in the **Transport** step, select the **tcp** or **udp** connector type and enable the **Auditd** toggle switch.

2 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Auditd events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

3 Configuring the event source server

You can configure the event source server using one of the following services:

rsyslog

The rsyslog service is used to transmit events from the server to the KUMA collector.

To configure transmission of events from the server to the collector:

1. Make sure that the rsyslog service is installed on the event source server. For this purpose, execute the following command:

   ```
   systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following command:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. Open the audit.service configuration file, /etc/audit/auditd.conf, and change the values of the following settings:

   ```
   name_format=NONE
   log_format=ENRICHED
   ```

   The `log_format` parameter determines the format of the records generated by the auditd service, and must be set to `ENRICHED` to have user information saved in events.

   After editing the settings, restart the auditd service:

   ```
   sudo systemctl restart auditd.service
   ```

3. In the `/etc/rsyslog.d` directory, create the audit.conf file with the following content, depending on your protocol:

   - To send events over TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/audit/audit.log
     $InputFileTag tag_audit_log:
     $InputFileStateFile audit_log
     $InputFileSeverity info
     $InputFileFacility local6
     $InputRunFileMonitor
     *.* @@<IP address of the KUMA collector>:<port of the KUMA collector>
     ```

     For example:

     ```
     *.* @@192.1.3.4:5858
     ```

- To send events over UDP:

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
template(name="AuditFormat" type="string" string="<%PRI%>%TIMESTAMP:::date-rfc3339% %HOSTNAME% %syslogtag%
%msg%")
*.* @<IP address of the KUMA collector>:<port of the KUMA collector>
```

```
For example:

*.* @192.1.3.4:5858;AuditFormat
```

4. Save the changes to the `audit.conf file`.

5. Restart the rsyslog service by executing the following command:

```
systemctl restart rsyslog.service
```

The event source server is configured. Data about events is transmitted from the server to the KUMA collector.

syslog-ng

The syslog-ng service is used to transmit events from the server to the KUMA collector.

To configure transmission of events from the server to the collector:

1. Make sure that the syslog-ng service is installed on the event source server by running the following command:

```
systemctl status syslog-ng.service
```

   If the syslog-ng service is not installed on the server, install the service by running one of the following commands depending on your package manager:

```
APT (Debian, Ubuntu)
```

```
apt install syslog-ng
```

```
YUM (CentOS 7, RHEL)
```

```
yum install syslog-ng
```

```
DNF (Fedora, CentOS 8)
```

```
dnf install syslog-ng
```

```
Zypper (openSUSE)
```

```
zypper install syslog-ng
```

```
Pacman (Arch Linux)
```

```
pacman -S syslog-ng
```

```
Snap (if available)
```

```
snap install syslog-ng
```

2. After installation, start the syslog-ng service:

```
systemctl enable syslog-ng.service
systemctl start syslog-ng.service
```

3. Open the /etc/audit/auditd.conf file of the audit.service service and change the value of the `name_format` setting to `NONE`:

```
name_format=NONE
```

4. After editing the settings, restart the auditd service:

```
sudo systemctl restart auditd.service
```

5. In the `/etc/syslog-ng directory, create the audit.conf file` with the following content, depending on your protocol:

```
To send events over TCP

source s_audit_log {
file("/var/log/audit/audit.log"
persist-name("s_audit_log_for_siem")
follow-freq(1)
program-override("auditd:")
flags(no-parse));
};
log {
source(s_audit_log);
destination(d_audit_log);
};
# Message formatting
template AuditFormat {
template("<${PRI}>${ISODATE} ${HOST} ${MSG}\n");
};
# Transferring audit logs to the specified KUMA collector address
destination d_audit_log {
tcp("<KUMA collector IP address>" port(<KUMA collector port>) persist-name("collector-audit")
template(AuditFormat));
};
```

```
To send events over UDP

source s_audit_log {
file("/var/log/audit/audit.log"
persist-name("s_audit_log_for_siem")
follow-freq(1)
program-override("auditd:")
flags(no-parse));
};
log {
source(s_audit_log);
destination(d_audit_log);
};
# Message formatting
template AuditFormat {
template("<${PRI}>${ISODATE} ${HOST} ${MSG}");
};
# Transferring audit logs to the specified KUMA collector address
destination d_audit_log {
udp("<KUMA collector IP address>" port(<KUMA collector port>) persist-name("collector-audit")
template(AuditFormat));
};
```

6. Save the changes to the `audit.conf file`.

7. Add the following string to `/etc/syslog-ng/syslog-ng.conf` configuration file:

```
@include " audit.conf "
```

8. Restart the syslog-ng service by executing the following command:

```
systemctl restart syslog-ng.service
```

The event source server is configured. Data about events is transmitted from the server to the KUMA collector.

4 Verifying receipt of Auditd events by the KUMA collector

To verify whether Auditd event source server is configured correctly, by searching for related events in the Kaspersky SIEM web interface.

FreeIPA

Configuring the receiving of FreeIPA events in Kaspersky SIEM via the Syslog protocol consists of the following steps:

1 Configuring export of FreeIPA events to KUMA

1. Connect to the FreeIPA server via SSH using an account with administrator rights.
2. In the `/etc/rsyslog.d/` directory, create a file named `freeipa-to-siem.conf`.

3. Add the following lines to the `/etc/rsyslog.d/freeipa-to-siem.conf` configuration file:

```
$ModLoad imfile
input(type="imfile"
      File="/var/log/httpd/error_log"
      Tag="tag_FreeIPA_log_httpd"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/audit"
      Tag="tag_FreeIPA_log_audit"
      StartMsg.regex="^time:"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/errors"
      Tag="tag_FreeIPA_log_errors"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/access"
      Tag="tag_FreeIPA_log_access"
      facility="local3")
input(type="imfile"
      File="/var/log/krb5kdc.log"
      Tag="tag_FreeIPA_log_krb5kdc"
      facility="local3")

template(name="ls_json" type="list" option.json="on") {
    constant(value="{")
    constant(value="\"@timestamp\":\"") property(name="timegenerated" dateFormat="rfc3339")
    constant(value="\",\"@version\":\"1")
    constant(value="\",\"message\":\"") property(name="msg")
    constant(value="\",\"host\":\"") property(name="fromhost")
    constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
    constant(value="\",\"logsource\":\"") property(name="fromhost")
    constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
    constant(value="\",\"severity\":\"") property(name="syslogseverity")
    constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
    constant(value="\",\"facility\":\"") property(name="syslogfacility")
    constant(value="\",\"program\":\"") property(name="programname")
    constant(value="\",\"pid\":\"") property(name="procid")
    constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
    constant(value="\"}\n")
}

if $syslogtag contains 'tag_FreeIPA_log' then {
    action(type="omfwd"
           target="<IP address of KUMA collector>"
           port="<port of KUMA collector>"
           protocol="<udp or tcp>"
           template="ls_json")
    stop
}
```

4. Add the following lines to the `/etc/rsyslog.conf` configuration file:

```
$IncludeConfig /etc/rsyslog.d/freeipa-to-siem.conf
$RepeatedMsgReduction off
```

5. If necessary, disable the local recording of FreeIPA events by doing the following:

   a. Open the `rsyslog /etc/rsyslog.conf` configuration file or the default rules file `/etc/rsyslog.d/50-default.conf` for editing.

   b. In that file, find the line that is responsible for recording system events, and add the `local3.none` option to it because in the `/etc/rsyslog.d/freeipa-to-siem.conf` configuration file, the `facility` is set to `local3`. The edited line should look like this:

   ```
   *.info;mail.none;authpriv.none;cron.none;local3.none    /var/log/messages
   ```

   If facility is set to `facility local3` for another application on the server, change the `facility` of FreeIPA in the `/etc/rsyslog.d/freeipa-to-siem.conf` file to a different value and edit the chosen `rsyslog` file accordingly.

   c. Save your changes.

6. Save changes to the `/etc/rsyslog.d/freeipa-to-siem.conf` configuration file.

7. Restart the rsyslog service by executing the following command:

   ```
   sudo systemctl restart rsyslog.service
   ```

2 Creating a KUMA collector for receiving FreeIPA events

To receive FreeIPA events, while creating a KUMA collector, select **[OOTB] FreeIPA** in the **Normalizer** field at the **Event parsing** step.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect FreeIPA events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of FreeIPA events by KUMA

To verify whether the FreeIPA event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

FreeRADIUS

You can configure the receipt of FreeRADIUS 3.0.26 events in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring audit of FreeRADIUS events

1. Connect to the server where the FreeRADIUS system is installed using an account with administrator rights.

2. Create a backup copy of the FreeRADIUS configuration file:

```
sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
```

3. Open the FreeRADIUS configuration file for editing:

```
sudo nano /etc/freeradius/3.0/radiusd.conf
```

4. In the 'log' section, edit the settings as follows:

```
destination = syslog
syslog_facility = daemon
stripped_names = no
auth = yes
auth_badpass = yes
auth_goodpass = yes
```

5. Save the configuration file.

FreeRADIUS event audit is configured.

2 Configuring a Syslog server to send FreeRADIUS events

The rsyslog service is used to transmit events from the FreeRADIUS server to the KUMA collector.

1. In the `/etc/rsyslog.d/` directory, create the `FreeRADIUS-to-siem.conf` file and add the following line to it:

```
If $programname contains 'radiusd' then @<IP address of the collector>:<port of the collector>
```

If you want to send events via TCP, the contents of the file must be as follows:

```
If $programname contains 'radiusd' then @<IP address of the collector>:<port of the collector>
```

2. Create a backup copy of the `/etc/rsyslog.conf` file.

3. Add the following lines to the `/etc/rsyslog.conf` configuration file:

```
$IncludeConfig /etc/FreeRADIUS-to-siem.conf
$RepeatedMsgReduction off
```

4. Save your changes.

5. Restart the rsyslog service:

```
sudo systemctl restart rsyslog.service
```

Transferring of events from the FreeRADIUS server to the KUMA collector is configured.

3 Creating a KUMA collector for receiving FreeRADIUS events

To receive FreeRADIUS events, while creating the collector, select the **[OOTB] FreeRADIUS syslog** normalizer at the **Event parsing** step, and select the **tcp** or **udp** connector type at the **Transport** step.

4 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect FreeRADIUS events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

5 Verifying receipt of FreeRADIUS events by the KUMA collector

To verify whether the FreeRADIUS event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

ProFTPD

Kaspersky SIEM enables monitoring of ProFTPD events on Linux devices. Events are collected and audited by ProFTPD, after which the events are sent to Kaspersky SIEM via the rsyslog syslog server.

Configuring the receipt of ProFTPD events involves the following steps:

1 Configuring audit of ProFTPD events.

1. Create a backup copy of the `/etc/proftpd/proftpd.conf` configuration file.

2. Open the `proftpd.conf` file and add or change the following settings:

```
LogFormat default "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
LogFormat auth "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
ExtendedLog /var/log/proftpd/access.log ALL default
ExtendedLog /var/log/proftpd/auth.log AUTH auth
```

3. Save changes and restart the service by running the following command:

```
sudo systemctl restart proftpd
```

Audit of ProFTPD events is configured.

ProFTPD does not perform log rotation. To reduce the risk of disk space filling up, we recommend using an external log rotation tool, such as Logrotate or Logadm.

2 Creating a KUMA collector for ProFTPD events

When creating a collector in the Kaspersky SIEM web interface, at the **Transport** step, you need to specify the port and protocol configured for the syslog server to send events. To receive audit events from ProFTPD, at the **Event parsing** step, select the **[OOTB] Proftpd syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect ProFTPD events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Configuring a syslog server to send events.

The rsyslog service is used to transmit events from the server to the KUMA collector.

1. Make sure that the rsyslog service is installed on the event source server. For this purpose, execute the following command:

   ```
   systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. In the /etc/rsyslog.d directory, create the proftpd.conf file with the following content, depending on your protocol:

   - To send events over TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<IP address of the KUMA collector>" port="<port of the KUMA collector>"
     protocol="tcp")
         stop
     }
     ```

   - To send events over UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<IP address of the KUMA collector>" port="<port of the KUMA collector>"
     protocol="udp")
         stop
     }
     ```

3. Save the changes to the `proftpd.conf` file.

4. Restart the rsyslog service by executing the following command:

   ```
   systemctl restart rsyslog.service
   ```

   The event source server is configured. Data about events is transmitted from the server to the KUMA collector.

5 Verifying receipt of ProFTPD events by the KUMA collector

To verify whether receipt of events from ProFTPD is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Vsftpd

Kaspersky SIEM enables monitoring of Vsftpd events on Linux devices. Events are collected and audited by Vsftpd, after which the events are sent to Kaspersky SIEM via the rsyslog syslog server.

Configuring the receipt of Vsftpd events involves the following steps:

1 Configuring audit of Vsftpd events.

1. Create a backup copy of the `/etc/vsftpd/vsftpd.conf` configuration file.

2. Open the `vsftpd.conf` file and add or change the values of the following parameters:

```
xferlog_enable=YES
xferlog_std_format=NO
xferlog_file=/var/log/vsftpd.log
log_ftp_protocol=YES
```

3. Save changes and restart the service by running the following command:

```
sudo systemctl restart vsftpd
```

Audit of Vsftpd events is configured.

Vsftpd does not perform log rotation. To reduce the risk of disk space filling up, we recommend using an external log rotation tool such as Logrotate or Logadm.

2 Creating a KUMA collector for Vsftpd events

When creating a collector in the KUMA web interface, at the **Transport** step, you need to specify the port and protocol configured for the syslog server to send events. To receive audit events from Vsftpd, at the **Event parsing** step, select the **[OOTB] Vsftpd syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Vsftpd events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Configuring a syslog server to send events.

The rsyslog service is used to transmit events from the server to the KUMA collector.

1. Make sure that the rsyslog service is installed on the event source server. For this purpose, execute the following command:

   ```
   systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. In the `/etc/rsyslog.d` directory, create the `vsftpd.conf` file with the following content, depending on your protocol:

   - To send events over TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @@<IP address of the KUMA collector>:<port of the KUMA collector>
     ```

     Example

     ```
     *.* @@192.1.3.4:5858
     ```

   - To send events over UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @<IP address of the KUMA collector>:<port of the KUMA collector>
     ```

     Example

     ```
     *.* @192.1.3.4:5858
     ```

3. Save the changes to the `vsftpd.conf` file.

4. Restart the rsyslog service by executing the following command:

   ```
   systemctl restart rsyslog.service
   ```

The event source server is configured. Data about events is transmitted from the server to the KUMA collector.

5 Verifying receipt of Vsftpd events by the KUMA collector

To verify whether receipt of events from Vsftpd is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

HAProxy

Kaspersky SIEM enables monitoring of events from HAProxy (version 2.4) load balancer in HTTP, TCP, HTTP CLF, Default, HTTPS (for version 2.6 and later), and TCP CLF (for version 3.2 and later) formats received via the syslog protocol.

Configuring the receipt of HAProxy events involves the following steps:

1 Configuring export of HAProxy events

1. Check the configuration file for any syntax errors by running the following command:

   ```
   haproxy -c -V -f /etc/haproxy/haproxy.cfg
   ```

   Possible messages when checking the configuration file

   If there are no syntax errors in the configuration file, HAProxy displays a notification `Configuration file is valid`.

   If any syntax errors are found in the configuration file, HAProxy tells you what the error is, for example:

   `[NOTICE] (284146): haproxy version is 2.4.24-0ubuntu0.22.04.2`

   `[NOTICE] (284146): path to executable is /usr/sbin/haproxy`

   `[ALERT] (284146): parsing [/etc/haproxy/haproxy.cfg:25] : unknown option 'httpdlog'; did you mean 'httplog' maybe ?`

   `[ALERT] (284146): Error(s) found in configuration file : /etc/haproxy/haproxy.cfg`

   `[ALERT] (284146): Fatal errors found in configuration`

   For more information about configuration file syntax, refer to the official documentation of HAProxy.

2. If the syntax check is successful, back up the original configuration file using the following command:

   ```
   sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy_backup.cfg
   ```

3. Open the `haproxy.cfg` configuration file by running the following command:

```
sudo vi /etc/haproxy/haproxy.cfg
```

The next steps of the instructions assume that the same logging settings are applied to all groups of servers. In this case, the logging settings are specified in the `global` section, and in the `defaults`, the `log global` line is used.

If you need a more granular logging configuration, you need to remove the `log global` line from the `defaults` section. Since the `frontend`, `backend`, and `listen` sections inherit parameters from the `defaults` section by default, this disables global logging. In this case, you need to specify logging settings in each section by adding a line of the following form:

```
log <IP_address_of_KUMA_collector> [len <length_in_bytes>] [format <syslog_message_format>] [sample <ranges>:
<sample_size>] <facility> [<level> [<minimum_level>]]
```

4. In the `global` section, specify the IP address of the KUMA collector:

```
log <collector_IP_address>:<port>
```

5. In the `global` section, add the following line to add the host name to the syslog header:

```
log-send-hostname <hostname>
```

6. In the `defaults` section, add a line to use global logging settings:

```
log global
```

7. In the `defaults` section, specify the logging format:

- For layer 4 balancers (TCP):

```
option tcplog
```

Example of a defaults section with settings

```
defaults
log global
mode tcp
option tcplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
```

- For layer 7 balancers (HTTP):

```
option httplog
```

Example of a defaults section with settings

```
defaults
log global
mode http
option httplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
```

8. If you want to enable logging of HTTP request headers, add the following line to the `frontend` or `listen` section:

```
capture request header <header_name> len <header_length_in_bytes>
```

Each header must be specified on a separate line, for example:

```
capture request header User-agent len 50
capture request header Host len 30
capture request header X-Forwarded-For len 15
```

9. If you want to enable logging of HTTP response headers, add the following line to the `frontend` or `listen` section:

```
capture response header <header_name> len <header_length_in_bytes>
```

Each header must be specified on a separate line, for example:

```
capture response header User-agent len 50
capture response header Host len 30
capture response header X-Forwarded-For len 15
```

10. If you want to enable logging of HTTP-cookie, add the following line to the `frontend` or `listen` section:

```
capture cookie <cookie_name> len <cookie_size_in_bytes>
```

Only the first cookie file with the specified name is logged.

11. Check the syntax of the configuration file for errors using the following command (see step 1 of the instructions):

```
haproxy -c -V -f /etc/haproxy/haproxy.cfg
```

12. Reload the configuration by running the following command:

```
sudo systemctl reload haproxy
```

13. Verify that the HAProxy load balancer has started and is operating normally by running the following command:

```
sudo systemctl status haproxy
```

Transferring of events from HAProxy is configured.

2 Creating a KUMA collector for receiving HAProxy events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] HAProxy syslog** normalizer, and at the **Transport** step, select the **udp** connector type.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect HAProxy events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of HAProxy events by the KUMA collector

To verify whether receipt of events from HAProxy is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Apache Tomcat

Kaspersky SIEM allows monitoring audit events of an Apache Tomcat web server version 9.0 and later, 10.1 and later, and 11.0 and later deployed on Linux devices. Events are collected and audited by Apache Tomcat, after which the events are sent to Kaspersky SIEM via the rsyslog syslog server.

Configuring Apache Tomcat event reception involves the following steps:

1 Configuring Apache Tomcat event audit

1. Connect to the Apache Tomcat server via SSH using an account with administrator rights.

> Further steps assume that the standard environment variables `$CATALINA_HOME` and `$JAVA_HOME` are configured on the server.

For more information on variables, see the Apache Tomcat installation guide.

2. Back up the original configuration file using the following command:

```
sudo cp $CATALINA_HOME/conf/server.xml $CATALINA_HOME/conf/server_backup.xml
```

3. Open the Apache Tomcat configuration file for editing using the following command:

```
sudo vi $CATALINA_HOME/conf/server.xml
```

4. Find the element `<Valve className="org.apache.catalina.valves.AccessLogValve" ... />` and replace it as follows to use `JsonAccessLogValve`:

```
<Valve className="org.apache.catalina.valves.JsonAccessLogValve" directory="logs"
prefix="access_log" suffix=".txt"
maxDays="7"
pattern="%h %a %t %m %U %q %r %H %A %v %p %s %b %X %I %{User-Agent}i %{Cookie}c"/>
```

If using `JsonAccessLogValve` is not possible, keep `AccessLogValve`, but set up an extended template to collect more fields:

```
pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocol=%H|localAddr=%A|localServerN
Agent=%{User-Agent}i|Cookie=%{Cookie}c"
```

```
Example configuration with AccessLogValve:

<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="access_log" suffix=".txt"
maxDays="7"
pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocol=%H|localAddr=%A|localServerN
Agent=%{User-Agent}i|Cookie=%{Cookie}c"/>
```

The normalizer also supports the Common and Combined templates for `AccessLogValve` and `JsonAccessLogValve`.

5. Restart the Apache Tomcat web server using the following commands:

```
sudo $CATALINA_HOME/bin/shutdown.sh
sudo $CATALINA_HOME/bin/startup.sh
sudo systemctl restart tomcat.service
```

Audit of Apache Tomcat events is configured.

2 Creating a KUMA collector for Apache Tomcat events.

When creating a collector in the Kaspersky SIEM web interface at the **Event parsing** step, select the **Apache Tomcat [OOTB]** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Apache Tomcat events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Configuring a syslog server to send events.

The rsyslog service is used to transmit events from the server to the KUMA collector.

1. Make sure that the rsyslog service is installed on the server that is the event source. For this purpose, execute the following command:

   ```
   systemctl status rsyslog.service
   ```

   If the service is running, a notification similar to the following is displayed:

   ```
   Active: active (running) since Tue 2025-09-23 15:31:30 MSK; 1 week 0 days ago
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   sudo apt install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. Check the syntax of the configuration file by running the following command:

   ```
   rsyslogd -N1
   ```

   Possible messages when checking the configuration file

   If there are no syntax errors in the configuration file, rsyslog displays the following notifications:

   ```
   rsyslogd: version 8.2112.0, config validation run (level 1), master config
   /etc/rsyslog.conf
   rsyslogd: End of config validation run. Bye.
   ```

   If any syntax errors are found in the configuration file, the rsyslog service tells you what the error is, for example:

   ```
   rsyslogd: version 8.2112.0, config validation run (level 1), master config
   /etc/rsyslog.conf
   rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
   https://www.rsyslog.com/e/2221 ]
   rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
   https://www.rsyslog.com/e/2221 ]
   rsyslogd: parameter "maxLinesAtOnce" not permited in inotify mode - ignored [v8.2112.0
   try https://www.rsyslog.com/e/2222 ]
   rsyslogd: $WorkDirectory: /var/lib/rsyslog not a directory - directive ignored
   [v8.2112.0 try https://www.rsyslog.com/e/2181 ]
   ```

```
rsyslogd: imfile: no working or state file directory set, imfile will create state
files in the current working directory (probably the root dir). Use
global(workDirectory="/some/path") to set the working directory [v8.2112.0 try
https://www.rsyslog.com/e/2450]
```

3. Open the `rsyslog.conf` configuration file by running the following command:

```
sudo vi /etc/rsyslog.conf
```

4. Confirm that the file includes a line that allows uploading configurations from the `/etc/rsyslog.d` directory by running the following commands:

```
# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")
```

5. Create the `apache_tomcat_to_siem.conf` configuration file in the `/etc/rsyslog.d/` directory by running the following command:

```
sudo touch /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

6. Open the created configuration file `apache_tomcat_to_siem.conf` using the following command:

```
sudo vi /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

7. Run the following command to find out the absolute path to the Apache Tomcat directory:

```
printenv CATALINA_HOME
```

You need to know the absolute path to specify it in the configuration file because the rsyslog service does not let you use environment variables.

8. Add the rules for reading the `Access Log` and for sending data to the KUMA collector to the configuration file:

```
input(
        type="imfile"
        File="<absolute_path_from_step_7>/logs/access_log*.txt"
        Tag="apachetomcat"
)

if $programname == "apachetomcat" then {
        action(
                type="omfwd"
                target="<FQDN_or_IP-address_of_a_KUMA_collector>"
                port="<KUMA_collector_port>"
                protocol="<udp_or_tcp>"
        )
}
```

9. Check the syntax of the configuration file for errors using the following command (see step 2 of the instructions):

```
rsyslogd -N1
```

10. Restart the rsyslog service by running the following command:

```
sudo systemctl restart rsyslog
```

11. Verify that the rsyslog service has started and is operating normally by running the following command:

```
sudo systemctl status rsyslog
```

Transferring of events from the server where the Apache Tomcat system is installed to the collector is configured.

5 Verifying receipt of Apache Tomcat events by the KUMA collector

To verify whether receipt of events from Apache Tomcat is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Network and security devices

This section describes how to configure the receiving of events from network devices and security systems.

IVK Kolchuga-K

You can configure the receipt of events from the IVK Kolchuga-K system to the Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring export of IVK Kolchuga-K events to KUMA

1. Connect to the firewall over SSH with administrator rights.

2. Create a backup copy of the `/etc/services` and `/etc/syslog.conf` files.

3. In the `/etc/syslog.conf` configuration file, specify the FQDN or IP address of the KUMA collector. For example:

```
*.* @kuma.example.com
```

or

```
*.* @192.168.0.100
```

4. Save changes to the configuration file `/etc/syslog.conf`.

5. In the /etc/services configuration file, specify the port and protocol used by the KUMA collector. For example:

```
syslog          10514/udp
```

6. Save changes to the `/etc/services` configuration file.

7. Restart the syslog server of the firewall:

```
service syslogd restart
```

2 Creating a KUMA collector for receiving events from IVK Kolchuga-K

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Kolchuga-K syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect IVK Kolchuga-K events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of IVK Kolchuga-K events by Kaspersky SIEM

To verify whether the IVK Kolchuga-K event source is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

CryptoPro NGate

You can configure the receipt of CryptoPro NGate events in the Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring export of CryptoPro NGate events to KUMA

1. Connect to the web interface of the NGate management system.
2. Connect remote syslog servers to the management system. To do so:
   a. Open the page with the list of syslog servers: **External Services** → **Syslog Server** → **Add Syslog Server**.
   b. Enter the settings of the syslog server and click ✔.
3. Assign syslog servers to the configuration for recording logs of the cluster. To do so:
   a. In the **Clusters** → **Summary** section, select the cluster that you want to configure**.**
   b. On the **Configurations** tab, click the **Configuration** control for the relevant cluster to go to the configuration settings page.
   c. In the **Syslog Servers** field of the configuration being configured, click **Assign**.
   d. Select the check boxes for syslog servers that you want to assign and click ✔.
      You can assign an unlimited number of servers.
      To add new syslog servers, click +.
   e. Publish the configuration to activate the new settings.
4. Link syslog servers
   to the management system for recording Administrator activity logs. To do so:
   a. Select the **Management Center Settings** menu item and on the page that is displayed, under **Syslog servers**, click **Assign**.
   b. In the **Assign Syslog Servers to Management Center** window, select the check box for those syslog servers that you want to assign, then click ✔.

   You can assign an unlimited number of servers.

CryptoPro NGate events will be sent to Kaspersky SIEM.

2 Creating a KUMA collector for receiving CryptoPro NGate events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] NGate syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

After creating and configuring the collector for reception of CryptoPro NGate events, install the KUMA Collector on the server of the network infrastructure intended for reception of events.

4 Verifying receipt of CryptoPro NGate events by the KUMA collector

To verify whether the CryptoPro NGate event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Ideco UTM

You can configure the receipt of Ideco UTM application events in KUMA via the Syslog protocol.

Configuring event receiving consists of the following steps:

1 Configuring export of Ideco UTM events to KUMA

1. Connect to the Ideco UTM web interface under a user account with administrator rights.
2. In the **System message forwarding** menu, move the **Syslog** toggle switch to the **enabled** position.
3. For the **IP address** setting, specify the IP address of the KUMA collector.
4. In the **Port** setting, specify the port that the KUMA collector is listening on.
5. Click **Save** to apply the changes.

Transferring of Ideco UTM events to KUMA is configured.

2 Creating a KUMA collector for receiving Ideco UTM events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Ideco UTM syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Ideco UTM events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Ideco UTM events by KUMA

To verify whether the Ideco UTM event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

McAfee Web Gateway

Configuring the receipt of events from the McAfee Web Gateway system (version 7.8) received via the Syslog protocol in the CEF format in Kaspersky SIEM consists of the following steps:

1 Creating an account in McAfee Web Gateway

Event export must be configured using an account with administrator rights.

1. In the McAfee Web Gateway web interface, open the **Policy** → **Rule Sets** section.
2. Click **Log Handler** in the lower part of the left pane of the web interface.
3. Find the required rule set, expand the **Default rule set**, and select the nested **CEF Syslog** rule set.

   The contents of the nested rule set are displayed in the configuration pane.
4. Turn on the **Send to Syslog** rule.
5. Click **Save changes**.
6. Configure the sending of audit log data via syslog. To do this, go to **Configuration** → **Appliances** → **Log File Manager** → **Settings**.
7. Select **Write audit log to syslog**.
8. To send data via syslog, change the settings in the `rsyslog.conf` syslog server configuration file as follows:

   a. Go to the **Configuration** → **File Editor** section.

   b. In the file tree, select the `rsyslog.conf` file.

      The contents of the file are be displayed in the configuration pane.

   c. Edit the rsyslog.conf file by replacing the string `*.info;mail.none;authpriv.none;cron.none /var/log/messages` with `*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages`.
9. Configure sending of data to a syslog server depending on the selected protocol by adding the following line to the end of the file:

   ```
   To send data over UDP:
   ```

   ```
   daemon.info @<syslog server address in x.x.x.x format>:<port number>
   ```

   ```
   To send data over TCP, add the following line to the end of the file:
   ```

   ```
   daemon.info @@<syslog server address in x.x.x.x format>:<port number>
   ```
10. Click **Save changes**.

2 Creating a KUMA collector to receive **McAfee Web Gateway** events

When creating a collector in KUMA at the **Event parsing** step, select the **[OOTB] McAfee Web Gateway** normalizer. At the **Transport** step, select either tcp or udp connector type depending on the configuration used for McAfee Web Gateway event transferring.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect McAfee Web Gateway events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of events from **McAfee Web Gateway** by the KUMA collector

To verify whether receipt of events from McAfee Web Gateway is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Positive Technologies Network Attack Discovery

You can configure event receiving from Positive Technologies Network Attack Discovery (hereinafter referred to as PT NAD) to the Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring the ptdpi-worker@notifier module for transferring PT NAD events to KUMA

To enable the sending of information about detected information security threats, you must configure the ptdpi-worker@notifier module.

In a multi-server configuration, these instructions must be followed on the primary server.

1. Open the `/opt/ptsecurity/etc/ptdpi.settings.yaml` file:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. In the `General settings` section, uncomment the `workers` parameter and add a `notifier` to its list of values.

   ```
   For example:
   workers: ad alert dns es hosts notifier
   ```

3. Add a line of the `notifier.yaml.nad_web_url: <URL of the PT NAD web interface>` form to the end of the file.

   For example:

   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```

   The `ptdpi-worker@notifier` module uses the specified URL to generate links to session and activity cards when sending messages.

4. Restart the sensor:

   ```
   sudo ptdpictl restart-all
   ```

The `ptdpi-worker@notifier` module will be configured.

2 Configuring the sending of syslog messages with information about activities, attacks and indicators of compromise

The settings listed in the following instructions may not be present in the configuration file. If a setting is missing, you must add it to the file.

In a multi-server PT NAD configuration, edit the settings on the primary server.

1. Open the `/opt/ptsecurity/etc/ptdpi.settings.yaml` file:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. By default, PT NAD sends activity information in Russian. To receive information in English, change the value of the `notifier.yaml.syslog_notifier.locale` setting to `en`.

   For example:

   ```
   notifier.yaml.syslog_notifier.locale: en
   ```

3. In the `notifier.yaml.syslog_notifier.addresses` option, add a section with parameters for sending events to Kaspersky SIEM.

   The `<Connection name>` option can only contain Latin letters, numerals, and the underscore character.

   In the `address` setting, specify the IP address of the KUMA collector. Other settings can be omitted, in which case the default values are used.

   ```
   notifier.yaml.syslog_notifier.addresses:
     <Connection name>:
           address: <For sending to a remote server, specify protocol: UDP (default) or TCP, address and port; for
   local connection, specify Unix domain socket>
           doc_types: [<Comma-separated message types ("alert" for information about attacks, "detection" for
   activities, and "reputation" for information about indicators of compromise). By default, all types of messages
   are sent>]
           facility: <Numeric value of the subject category>
           ident: <software tag>
   ```

```
  <Connection name>:
        ...
```

Example configuration of sending syslog messages with information about activities, attacks, and indicators of compromise to two remote servers via TCP and UDP without writing to the local log

```
notifier.yaml.syslog_notifier.addresses:
  remote1:
    address: tcp://198.51.100.1:1514
  remote2:
    address: udp://198.51.100.2:2514
```

4. Save your changes to the `/opt/ptsecurity/etc/ptdpi.settings.yaml` file.

5. Restart the ptdpi-worker@`notifier` module:

```
sudo ptdpictl restart-worker notifier
```

Sending of events to Kaspersky SIEM via Syslog is configured.

❸ Creating a KUMA collector for receiving PT NAD events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] PT NAD json** normalizer.

❹ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect PT NAD events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❺ Verifying receipt of PT NAD events by the KUMA collector

To verify whether the PT NAD event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Snort

You can configure the receipt of Snort 3 events in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring logging of Snort events

Make sure that the server running Snort has at least 500 MB of free disk space for storing a single Snort event log.
When the log reaches 500 MB, Snort automatically creates a new file with a name that includes the current time in unixtime format.
We recommend monitoring disk space usage.

1. Connect to the server where Snort is installed using an account with administrator rights.

2. Edit the Snort configuration file. To do so, run the following command on the command line:

```
sudo vi /usr/local/etc/snort/snort.lua
In the configuration file, edit the alert_json block's content:
alert_json =
{
file = true,
limit = 500,
fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls \
pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
}
```

3. To complete the configuration, run the following command:

```
sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l /var/log/snort -i <name of the
interface that Snort is listening on> -m 0x1b
```

Snort events will be logged to `/var/log/snort/alert_json.txt`.

2 Creating a KUMA collector for receiving Snort events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Snort 3 json file** normalizer, and at the **Transport** step, select the **file** connector type.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Snort events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Snort events by the KUMA collector

To verify whether the Snort event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Suricata

Configuring the receiving of events from Suricata version 7.0.1 in Kaspersky SIEM consists of the following steps:

1 Configuring export of Suricata events to KUMA

1. Connect via SSH to the server that has administrative user accounts.
2. Create a backup copy of the `/etc/suricata/suricata.yaml` file.

```
Set the following values in the eve-log section of the /etc/suricata/suricata.yaml configuration file:
- eve-log:
  enabled: yes
  filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
  filename: eve.json
```

3. Save your changes to the `/etc/suricata/suricata.yaml` configuration file.

   Suricata events will be logged to the `/usr/local/var/log/suricata/eve.json` file.

Suricata does not support limiting the size of the `eve.json` event file. If necessary, you can manage the log size by using rotation. For example, to configure hourly log rotation, add the following lines to the configuration file:

```
outputs:
  - eve-log:
    filename: eve-%Y-%m-%d-%H:%M.json
    rotate-interval: hour
```

2 Creating a KUMA collector for receiving Suricata events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Suricata json file** normalizer, and at the **Transport** step, select the **file** connector type.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Suricata events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Suricata events by the KUMA collector

To verify whether the Suricata event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

zVirt

You can configure the receipt of zVirt 3.1 events in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring the export of zVirt events to KUMA

ZVirt can send events to external systems in Hosted Engine installation mode.

1. In the zVirt web interface, under **Resources**, select **Virtual machines**.
2. Select the computer that is running the HostedEngine virtual machine and click **Edit**.
3. In the **Edit virtual machine** window, go to the **Logging** section.
4. Select the **Determine Syslog server address** check box.
5. In the text box, enter the collector information in the following format: `<IP address or FQDN of the KUMA collector>:<port of the KUMA collector>`.
6. If you want to use TCP instead of UDP for sending logs, select the **Use TCP connection** check box.

Transferring of events is configured.

2 Creating a KUMA collector for receiving zVirt events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] OrionSoft zVirt syslog** normalizer, and at the **Transport** step, select the **tcp** or **udp** connector type.

3 Installing the KUMA collector in the network infrastructure

Once you configured the collector for receiving zVirt events, install the KUMA collector on the server of the network infrastructure intended for receiving events.

4 Verifying receipt of zVirt events by the KUMA collector

To verify whether the zVirt event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

ViPNet TIAS

You can configure the receipt of ViPNet TIAS events in KUMA via the Syslog protocol.

Configuring event receiving consists of the following steps:

1 Configuring export of ViPNet TIAS events to KUMA

1. Connect to the ViPNet TIAS web interface under a user account with administrator rights.
2. Go to the **Management** – **Integrations** section.
3. On the **Integration** page, switch to the **Syslog** tab.
4. In the toolbar of the list of receiving servers, click **New server**.
5. This opens the new server card; in that card:
   a. In the **Server address** field, enter the IP address or domain name of the KUMA collector, e. g., `10.1.2.3` or `syslog.siem.ru`.
   b. In the **Port** field, specify the inbound port of the KUMA collector. The default port number is 514.
   c. In the **Protocol** list, select the transport layer protocol that the KUMA collector is listening on. UDP is selected by default.
   d. In the **Organization** list, use the check boxes to select the organizations of the ViPNet TIAS infrastructure.

      Messages are sent only for incidents detected based on events received from sensors of selected organizations of the infrastructure.
   e. In the **Status** list, use check boxes to select incident statuses.

      Messages are sent only when selected statuses are assigned to incidents.
   f. In the **Severity level** list, use check boxes to select the severity levels of the incidents.

      Messages are sent only about incidents with the selected severity levels. By default, only the high severity level is selected in the list.
   g. In the **UI language** list, select the language in which you want to receive information about incidents in messages. Russian is selected by default.
6. Click **Add**.

7. In the toolbar of the list, enable the **Do not send incident information in CEF format** toggle switch.

   When new incidents are detected or the statuses of previously detected incidents change, depending on the statuses selected during configuration, the corresponding information is sent to the specified addresses of receiving servers via the syslog protocol in CEF format.

8. Click **Save changes**.

Sending of events to the KUMA collector is configured.

❷ Creating a KUMA collector for receiving ViPNet TIAS events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Syslog CEF** normalizer.

❸ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect ViPNet TIAS events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❹ Verifying receipt of ViPNet TIAS events by Kaspersky SIEM

To verify whether the ViPNet TIAS event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Zeek IDS

You can configure the receipt of Zeek IDS 1.8 events in the KUMA SIEM system.

Configuring event receiving consists of the following steps:

❶ Conversion of the Zeek IDS event log format

By default, Zeek IDS events are logged in files in the `/opt/zeek/logs/current` directory.

The "[OOTB] ZEEK IDS json file" normalizer supports Zeek IDS logs in the JSON format. To send events to the KUMA normalizer, log files must be converted to the JSON format.

> This procedure must be repeated every time before receiving Zeek IDS events.

1. Connect to the server where Zeek IDS is installed using an account with administrator rights.
2. Create the directory where JSON event logs must be stored:

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. Change to this directory:

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. Run the command that uses the jq utility to convert the original event log format to the target format:

   ```
   jq . -c <path to the log file to be converted to a different format> >> <new file name>.log
   ```

   ```
   Example:
   jq . -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

   A new file is created in the `/opt/zeek/logs/zeek-json` directory if this file did not exist before. If the file was already present in the current directory, new information is appended to the end of the file.

2 Creating a KUMA collector for receiving Zeek IDS events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] ZEEK IDS json file** normalizer, and at the **Transport** step, select the **file** connector type.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Zeek IDS events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Zeek IDS events by the KUMA collector

To verify whether the Zeek IDS event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Angie

Kaspersky SIEM enables monitoring of audit events from Angie or Angie Pro web server (version 1.10.1 or later) that is deployed on Linux devices.

Configuring the sending and receipt of events involves the following steps:

1 Configuring the export of Angie events

1. Check the configuration file for any syntax errors by running the following command:

   ```
   sudo angie -t
   ```

   Possible messages when checking the configuration file

   If there are no syntax errors in the configuration file, Angie displays the following notifications:

   ```
   angie: the configuration file /etc/angie/angie.conf syntax is ok
   angie: configuration file /etc/angie/angie.conf test is successful
   ```

   If any syntax errors are found in the configuration file, Angie tells you what the error is, for example:

   ```
   angie: [emerg] "http" directive is not allowed here in etc/angie/http.d/angie-to-siem.conf:1
   angie: configuration file /etc/angie/angie.conf test failed
   ```

   For more information about configuration file syntax, refer to the official documentation of Angie.

2. If the syntax check is successful (the result is `test is successful`), back up the original configuration file using the following command:

   ```
   sudo cp /etc/angie/angie.conf /etc/angie/angie_backup.conf
   ```

3. Open the `angie.conf` configuration file by running the following command:

   ```
   sudo vi /etc/angie/angie.conf
   ```

   By default, the standard `angie.conf` configuration file is stored in the `/etc/angie` directory.

   If a non-standard configuration file is used in the operation of the Angie web server, you must open that file. You can locate this file using the following command:

   ```
   sudo angie -V
   ```

   The location of the file is specified in the `--config-path` option.

4. Make sure that in the `http` context, the `include` directive is specified, which allows managing configuration using child configuration files, by running the following command:

```
include /etc/angie/http.d/*.conf
```

5. Create the `angie-to-siem.conf` configuration file in the `/etc/angie/http.d/` directory by running the following command:

```
touch /etc/angie/http.d/angie-to-siem.conf
```

6. Open the `angie-to-siem.conf` configuration file by running the following command:

```
sudo vi /etc/angie/http.d/angie-to-siem.conf
```

7. In the `log_format` directive, specify the format of the events to be sent as follows:

```
log_format syslog
device_event_category=access_log|time=$time_iso8601|version=$angie_version|http_method=$request_method|req_body=$r
```

8. In the `access_log` directive, specify the method to be used to send event information via Syslog:

```
access_log syslog:server=<collector_IP>:<port> syslog
```

9. If you also need to send information about events with errors, add a line with the `error_log` directive:

```
error_log syslog:server=<collector_IP>:<port>
```

The message format from the `error_log` directive cannot be changed; the message is always sent in the following form:

```
YYYY/MM/DD HH:MM:SS [LEVEL] PID#TID: *CID MESSAGE
```

Where:

- `YYYY/MM/DD` is the date in the year/month/day format.
- `HH:MM:SS` is the time in the hours:minutes:seconds format.
- `[LEVEL]` is the error severity level.
- `PID#TID` is the process ID (PID) and thread ID (TID).
- `*CID` is the unique connection number (Connection ID).
- `MESSAGE` is the text of the error or warning message.

10. Check the syntax of the configuration file for errors using the following command (see step 1 of the instructions):

```
sudo angie -t
```

11. Reload the configuration by running the following command:

```
sudo service angie reload
```

Sending of events from Angie is configured.

❷ Creating a KUMA collector for Angie events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Angie syslog** normalizer.

❸ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Angie events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❹ Verifying receipt of Angie events by the KUMA collector

To verify whether receipt of events from Angie and Angie Pro is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Dallas Lock 8

Kaspersky SIEM enables monitoring of events from Dallas Lock 8 version 11.4.2 system that are received in CEF format.

Configuring event receiving consists of the following steps:

1 Configuring the export of Dallas Lock 8 events

1. In Dallas Lock 8, go to **Download logs** menu.
2. Select the **Export logs to SIEM system** check box and do the following:
   a. In the **Server** field, enter the IP address or FQDN of the KUMA collector.
   b. In the **Port** field, specify the port that the KUMA collector is listening on.
   c. Select the **CEF** download format.
   d. Select **UTF-8** download encoding.
3. Select the check boxes next to the types of events that you want to send to KUMA.
4. In the **Log download period** drop-down list, select **1 minute**.
5. Click **OK**.

Event export is configured.

2 Creating a KUMA collector for Dallas Lock 8 events.

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Confident Dallas Lock syslog CEF** normalizer. Also, on the **Transport** tab, specify the same port and protocol that were configured for event sending.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Dallas Lock 8 events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Dallas Lock 8 events by the KUMA collector

To verify whether the Dallas Lock 8 event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Dallas Lock Unified Control Center

Kaspersky SIEM enables monitoring of events from Dallas Lock Unified Control Center 4.0 (hereinafter referred to as Dallas Lock UCC) that are received in CEF format.

Configuring event receiving consists of the following steps:

1. Configuring the export of Dallas Lock UCC events

1. In the Dallas Lock UCC, go to the **Export security incidents** menu.
2. Select the **Export security incidents to SIEM system** check box and do the following:
   a. In the **Format** drop-down list, select the **CEF** format.
   b. In the **Server** field, enter the IP address or FQDN of the KUMA collector.
   c. In the **Protocol** field, specify the communication protocol.
   d. In the **Port** field, specify the port that the KUMA collector is listening on.
3. Click **Apply**.

Sending of events is configured.

2. Creating a KUMA collector for Dallas Lock UCC events

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Confident Dallas Lock syslog CEF** normalizer. Also, on the **Transport** tab, specify the same port and protocol that were configured for event sending.

3. Installing the KUMA collector in the network infrastructure

Once you configured the collector for collecting Dallas Lock UCC events, install the KUMA collector on the server of the network infrastructure intended for receiving events.

4. Verifying receipt of Dallas Lock UCC events by the KUMA collector

To verify whether the Dallas Lock UCC event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Database and DBMS audit systems

This section describes how to configure the receiving of DBMS events and database audit plugins.

PostgreSQL

Kaspersky SIEM enables monitoring and audit of PostgreSQL events on Linux devices using rsyslog.

Events are audited using the pgAudit plugin. The plugin supports PostgreSQL 9.5 and later. For details about the pgAudit plugin, see https://github.com/pgaudit/pgaudit.

Configuring event receiving consists of the following steps:

1 Installing the pdAudit plugin

1. On the OS command line, run the following commands as a user with administrator rights:

```
sudo apt update
sudo apt -y install postgresql-<PostgreSQL version>-pgaudit
```

   You must select the plugin version to match the PostgresSQL version. For information about PostgreSQL versions and the matching plugin versions, see https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

```
For example:

sudo apt -y install postgresql-12-pgaudit
```

2. Find the `postgres.conf` configuration file. To do so, run the following command on the PostgreSQL command line:

```
show data_directory
```

   The response will indicate the location of the configuration file.

3. Create a backup copy of the `postgres.conf` configuration file.

4. Open the `postgres.conf` file and copy or replace the values in it with the values listed below.

```
## pgAudit settings
shared_preload_libraries = 'pgaudit'
## database logging settings
log_destination = 'syslog'
## syslog facility
syslog_facility = 'LOCAL0'
## event ident
syslog_ident = 'Postgres'
## sequence numbers in syslog
syslog_sequence_numbers = on
## split messages in syslog
syslog_split_messages = off
## message encoding
lc_messages = 'en_US.UTF-8'
## min message level for logging
client_min_messages = log
## min error message level for logging
log_min_error_statement = info
## log checkpoints (buffers, restarts)
log_checkpoints = off
## log query duration
log_duration = off
## error description level
log_error_verbosity = default
## user connections logging
log_connections = on
## user disconnections logging
log_disconnections = on
## log prefix format
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status. dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

5. Restart the PostgreSQL service using the command:

```
sudo systemctl restart postgresql
```

6. Load the pgAudit plugin in PostgreSQL. To do so, run the following command on the PostgreSQL command line:

```
CREATE EXTENSION pgaudit;
```

The pgAudit plugin is installed.

2 Creating a KUMA collector for receiving PostgreSQL events

To receive PostgreSQL events using rsyslog during the collector creation, select the **[OOTB] PostgreSQL pgAudit syslog** normalizer at the **Event parsing** step.

3 Installing the KUMA collector in the network infrastructure

After creating and configuring the collector for reception of PostgreSQL events, install the KUMA collector on the server of the network infrastructure intended for reception of events.

4 Configuring a Syslog server to send events

The rsyslog service is used to transfer events from the server to Kaspersky SIEM.

1. To verify that the rsyslog service is installed on the event source server, run the following command as administrator:

   ```
   sudo systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. In the `/etc/rsyslog.d/` directory, create a `pgsql-to-siem.conf` file with the following content:

   ```
   If $programname contains 'Postgres' then @<IP address of the collector>:<port of the collector>
   ```

   ```
   For example:
   ```

   ```
   If $programname contains 'Postgres' then @192.168.1.5:1514
   ```

   If you want to send events via TCP, the contents of the file must be as follows:

   ```
   If $programname contains 'Postgres' then @@<IP address of the collector>:<port of the collector>
   ```

3. Save changes to the `pgsql-to-siem.conf` configuration file.

4. Add the following lines to the `/etc/rsyslog.conf` configuration file:

   ```
   $IncludeConfig /etc/pgsql-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Save changes to the `/etc/rsyslog.conf` configuration file.

6. Restart the rsyslog service by executing the following command:

   ```
   sudo systemctl restart rsyslog.service
   ```

5 Verifying receipt of PostgreSQL events by the KUMA collector

To verify whether the PostgreSQL event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

MariaDB Audit Plugin

Kaspersky SIEM allows auditing events using the MariaDB Audit Plugin. The plugin supports MySQL 5.7 and MariaDB. The audit plugin does not support MySQL 8. Detailed information about the plugin is available on the official MariaDB website.

> We recommend using MariaDB Audit Plugin version 1.2 or later.

Configuring event receiving consists of the following steps:

1 Configuring the MariaDB Audit Plugin

You can configure event transfer using the MariaDB Audit Plugin using one of the following instructions:

To transfer MySQL events

The MariaDB Audit Plugin is supported for MySQL 5.7 versions up to 5.7.30 and is bundled with MariaDB.

To configure MySQL 5.7 event reporting using the MariaDB Audit Plugin:

1. Download the MariaDB distribution kit and extract it.

   You can download the MariaDB distribution kit from the official MariaDB website. The operating system of the MariaDB distribution must be the same as the operating system on which MySQL 5.7 is running.

2. Connect to MySQL 5.7 using an account with administrator rights by running the following command:

   ```
   mysql -u <username> -p
   ```

3. To get the directory where the MySQL 5.7 plugins are located, on the MySQL 5.7 command line, run the following command:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

4. In the directory obtained at step 3, copy the MariaDB Audit Plugin from `<directory to which the distribution kit was extracted>/mariadb-server-<version>/lib/plugins/server_audit.so`.

5. On the operating system command line, run the following command:

```
chmod 755 <directory to which the distribution kit was extracted>server_audit.so
```

```
For example:

chmod 755 /usr/lib64/mysql/plugin/server_audit.so
```

6. On the MySQL 5.7 command line, run the following command:

   `install plugin server_audit soname 'server_audit.so'`

7. Create a backup copy of the `/etc/mysql/mysql.conf.d/mysqld.cnf` configuration file.

8. In the configuration file `/etc/mysql/mysql.conf.d/mysqld.cnf`, in the `[mysqld]` section, add the following lines:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   If you want to disable event export for certain audit event groups, remove some of the values from the `server_audit_events` setting. Descriptions of settings are available on the MariaDB Audit Plugin vendor's website.

9. Save changes to the configuration file.

10. Restart the MariaDB service by running one of the following commands:

    - `systemctl restart mysqld` for a system with systemd initialization.
    - `service mysqld restart` for a system with init initialization.

MariaDB Audit Plugin for MySQL 5.7 is configured. If necessary, you can run the following commands on the MySQL 5.7 command line:

- `show plugins` to review the list of current plug-ins.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` to review the current audit settings.

To transfer MariaDB events

The MariaDB Audit Plugin is included in the MariaDB distribution kit starting with versions 5.5.37 and 10.0.10.

To configure MariaDB event export using the MariaDB Audit Plugin:

1. Connect to MariaDB using an account with administrator rights by running the following command:

   ```
   mysql -u <user name> -p
   ```

2. To check if the plugin is present in the directory where operating system plugins are located, run the following command on the MariaDB command line:

```
SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
```

3. On the operating system command line, run the following command:

```
ll <directory obtained by the previous command output> | grep server_audit.so
```

If the command output is empty and the plugin is not present in the directory, you can either copy the MariaDB Audit Plugin to that directory or use a newer version of MariaDB.

4. On the MariaDB command line, run the following command:

```
install plugin server_audit soname 'server_audit.so'
```

5. Create a backup copy of the `/etc/mysql/my.cnf` configuration file.

6. In the `/etc/mysql/my.cnf` configuration file, in the `[mysqld]` section, add the following lines:

```
server_audit_logging=1
server_audit_events=connect,table,query_ddl,query_dml,query_dcl
server_audit_output_type=SYSLOG
server_audit_syslog_facility=LOG_SYSLOG
```

If you want to disable event export for certain audit event groups, remove some of the values from the `server_audit_events` setting. Descriptions of settings are available on the MariaDB Audit Plugin vendor's website.

7. Save changes to the configuration file.

8. Restart the MariaDB service by running one of the following commands:

   - `systemctl restart mariadb` for a system with systemd initialization.

   - `service mariadb restart` for a system with init initialization.

MariaDB Audit Plugin for MariaDB is configured. If necessary, you can run the following commands on the MariaDB command line:

- `show plugins` to review the list of current plug-ins.

- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` to review the current audit settings.

2 Creating a KUMA collector for MySQL 5.7 and MariaDB events

To receive MySQL 5.7 and MariaDB events using the MariaDB Audit Plugin, during creation of the KUMA collector, in the **Normalizer** field, select **[OOTB] MariaDB Audit Plugin syslog** at the **Event parsing** step.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect MySQL 5.7 or MariaDB events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Configuring a Syslog server to send events

The rsyslog service is used to transmit events from the server to the collector.

1. Before making any changes, create a backup copy of the `/etc/rsyslog.conf` configuration file.
2. To send events via UDP, add the following line to the `/etc/rsyslog.conf` configuration file:

   ```
   *.* @<IP address of the KUMA collector>:<port of the KUMA collector>
   ```

   ```
   For example:
   *.* @192.168.1.5:1514
   ```

   If you want to send events over TCP, the line should be as follows:

   ```
   *.* @@192.168.1.5:2514
   ```

3. Save changes to the `/etc/rsyslog.conf` configuration file.
4. Restart the rsyslog service by executing the following command:

   ```
   sudo systemctl restart rsyslog.service
   ```

5 Verifying receipt of MySQL and MariaDB events by the KUMA collector

To verify that the MySQL and MariaDB event source server is configured correctly, you can search for related events.

Apache Cassandra

Kaspersky SIEM enables reception of data about Apache Cassandra events.

Configuring event receiving consists of the following steps:

1 Configuring Apache Cassandra event logging in KUMA

1. Make sure that the server where Apache Cassandra is installed has 5 GB of free disk space.

2. Connect to the Apache Cassandra server using an account with administrator rights.

3. Before making changes, create backups of the following configuration files: `/etc/cassandra/cassandra.yaml` and `/etc/cassandra/logback.xml`.

4. Make sure that the settings in the `/etc/cassandra/cassandra.yaml` configuration file have the following values; make changes if necessary:

   a. In the `audit_logging_options` section, set the `enabled` setting to `true`.

   b. In the `logger` section, set the `class_name` setting to `FileAuditLogger`.

5. Add the following lines to the `/etc/cassandra/logback.xml` configuration file:

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${cassandra.logdir}/audit/audit.log</file>
 <rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <!-- rollover daily -->
    <fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-dd}.%i.zip</fileNamePattern>
    <!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB -->
    <maxFileSize>50MB</maxFileSize>
    <maxHistory>30</maxHistory>
    <totalSizeCap>5GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', ' '}%n</pattern>
  </encoder>
</appender>

<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
    <appender-ref ref="AUDIT"/>
</logger>
```

6. Save changes to the configuration file.

7. Restart the Apache Cassandra service using the following commands:

```
sudo systemctl stop cassandra.service
```

```
sudo systemctl start cassandra.service
```

8. After restarting, check the status of Apache Cassandra using the following command:

```
sudo systemctl status cassandra.service
```

   Make sure that the command output contains the following sequence of characters:

```
Active: active (running)
```

Apache Cassandra event export is configured. Events are located in the `/var/log/cassandra/audit/directory`, in the `audit.log` file (`${cassandra.logdir}/audit/audit.log`).

2 Creating a KUMA collector for Apache Cassandra events

To receive Apache Cassandra events, perform the following steps while creating a KUMA collector: select a **file** type connector at the **Transport** step; select **[OOTB] Apache Cassandra file** in the **Normalizer** field at the **Event parsing** step.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Apache Cassandra events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Apache Cassandra events by the KUMA collector

To verify whether the Apache Cassandra event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Cloud and virtual platforms

This section describes how to configure the receiving of events from cloud platforms, virtual machines, and backup systems.

Nextcloud

You can configure the receipt of Nextcloud 26.0.4 events in Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring audit of Nextcloud events

1. On the server where Nextcloud is installed, create a backup copy of the `/home/localuser/www/nextcloud/config/config.php` configuration file.

2. Edit the `/home/localuser/www/nextcloud/config/config.php` Nextcloud configuration file.

3. Edit the settings as follows:

```
    'log_type' => 'syslog',
    'syslog_tag' => 'Nextcloud',
    'logfile' => '',
    'loglevel' => 0,
    'log.condition' => [
        'apps' => ['admin_audit'],
    ],
```

4. Restart the Nextcloud service:

```
sudo service restart nextcloud
```

Export of events to the KUMA collector is configured.

2 Configuring a Syslog server to send events

The rsyslog service is used to transmit events from the server to the collector.

1. In the `/etc/rsyslog.d/` directory, create a `Nextcloud-to-siem.conf` file with the following content:

```
If $programname contains 'Nextcloud' then @<IP address of the collector>:<port of the collector>
```

```
Example:
If $programname contains 'Nextcloud' then @192.168.1.5:1514
```

If you want to send events via TCP, the contents of the file must be as follows:

```
If $programname contains 'Nextcloud' then @<IP address of the collector>:<port of the collector>
```

2. Save changes to the `Nextcloud-to-siem.conf` configuration file.

3. Create a backup copy of the `/etc/rsyslog.conf` file.

4. Add the following lines to the `/etc/rsyslog.conf` configuration file:

```
$IncludeConfig /etc/Nextcloud-to-siem.conf
$RepeatedMsgReduction off
```

5. Save your changes.

6. Restart the rsyslog service by executing the following command:

```
sudo systemctl restart rsyslog.service
```

The export of Nextcloud events to the collector is configured.

3 Creating a KUMA collector for receiving Nextcloud events

To receive Nextcloud events, while creating the collector select the **[OOTB] Nextcloud syslog** normalizer at the **Event parsing** step, and select the **tcp** or **udp** connector type at the **Transport** step.

4 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Nextcloud events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

5 Verifying receipt of Nextcloud events by the KUMA collector

To verify whether the Nextcloud event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Yandex Cloud

Configuring the receiving of events from the Yandex Cloud system in Kaspersky SIEM consists of the following steps:

1 Configuring audit of Yandex Cloud events

Configuring event export involves the following steps:

1. Preparing the environment for working with Yandex Cloud.

To manage the configuration, you need Yandex Cloud CLI; install and initialize it.

Note: by default, audit is performed in the Yandex Cloud folder specified in the CLI profile. You can specify a different folder using the `--folder-name` or `--folder-id` parameter.

To configure the audit, you need an active billing account because a fee is charged for using the Yandex Cloud infrastructure.

To configure Yandex Cloud audit, you need an active billing account:

1. Go to the management console, then log in to Yandex Cloud or register.
2. On the Yandex Cloud Billing page, make sure that you have a billing account connected and that it has the ACTIVE or TRIAL_ACTIVE status. If you do not have a billing account, create one.

If you have an active billing account, you can create or select a Yandex Cloud folder in which your infrastructure will work, on the cloud page.

2. Creating a bucket for audit logs

To create a bucket:

1. In the management console, go to the folder in which you want to create the bucket, for example, **example-folder**.
2. Select the **Object Storage** service.
3. Click **Create bucket**.
4. On the bucket creation page:
   a. Enter the bucket name in accordance with the naming rules, for example **kumabucket**.
   b. If necessary, limit the maximum size of the bucket. Size 0 means no limit and is equivalent to the enabled **No limit** option.
   c. Select the type of access: **Restricted**.
   d. Select the default storage class.
   e. Click **Create bucket**.

   The bucket is created.

3. Creating an encryption key in the Key Management Service

To create an encryption key:

1. In the management console, go to the **example-folder** folder.
2. Select the **Key Management Service**.
3. Click the **Create key** button and specify the following settings:
   - Name (for example, **kuma-kms**).
   - Encryption algorithm, **AES-256**.
   - Keep default values for the rest of the settings.
4. Click **Create**.

   The encryption key is created.

4. Enabling bucket encryption

To enable bucket encryption:

1. In the management console, go to the bucket you created earlier.
2. In the left pane, select **Encryption**.

3. In the **KMS key** field, select the **kuma-kms** key.

4. Click **Save**.

Bucket encryption is enabled.

5. Creating service accounts

To create service accounts (a separate account for the trail and a separate account for the bucket):

1. Create the **sa-kuma** service account:

    1. In the management console, go to the **example-folder** folder.

    2. In the upper part of the scree, go to the **Service accounts** tab.

    3. Click **Create service account** and enter the name of the service account, for example, **sa-kuma**, making sure the name complies with the naming rules:

        - length: 3 to 63 characters

        - may contain lowercase letters of the Latin alphabet, numerals, and hyphens

        - the first character must be a letter, the last character may not be a hyphen.

    4. Click **Create**.

2. Create the **sa-kuma-bucket** service account:

    1. In the management console, go to the **example-folder** folder.

    2. In the upper part of the scree, go to the **Service accounts** tab.

    3. Click **Create service account** and enter the name of the service account, for example, **sa-kuma-bucket**, making sure the name complies with the naming rules:

        - length: 3 to 63 characters

        - may contain lowercase letters of the Latin alphabet, numerals, and hyphens

        - the first character must be a letter, the last character may not be a hyphen.

    4. Click **Create**.

The service accounts are created.

6. Creating a static key

You will need the key ID and the private key when mounting the bucket. You can create a key using the management console or the CLI.

To create a key using the management console:

1. In the management console, go to the **example-folder** folder.

2. In the upper part of the screen, go to the **Service accounts** tab.

3. Select the **sa-kuma-bucket** service account and click the row with its name.

4. In the upper panel, click **Create new key**.

5. Select **Create static access key**.

6. Enter a description for the key and click **Create**.

7. Save the ID and the secret key.

The static access key is created. The key value will become unavailable when you close the dialog.

To create a key using the CLI:

1. Create an access key for the **sa-kuma-bucket** service account:

```
yc iam access-key create --service-account-name sa-kuma-bucket
```

Result:

```
access_key:
  id: aje*******k2u
  service_account_id: aje*******usm
  created_at: "2022-09-22T14:37:51Z"
  key_id: 0n8*******0YQ
secret: JyT*******zMP1
```

2. Save the key_id and the key from the 'secret' value. You will not be able to get the key value again.

The access key is created.

7. Assigning roles to service accounts

To assign the audit-trails.viewer, storage.uploader, and kms.keys.encrypterDecrypter roles to the sa-kuma service account:

1. In the CLI, assign the audit-trails.viewer role to the folder:

```
yc resource-manager folder add-access-binding \
--role audit-trails.viewer \
--id <directory_id> \
--service-account-id <service_account_id>
```

Where:

- `--role` is the assigned role.
- `--id` is the ID of the 'example-folder' folder.
- `--service-account-id` is the ID of the sa-kuma service account.

2. Assign the storage.uploader role to the folder with the bucket:

```
yc resource-manager folder add-access-binding \
--role storage.uploader \
```

```
--id <directory_id> \
--service-account-id <service_account_id>
```

Where:

- `--role` is the assigned role.
- `--id` is the ID of the 'example-folder' folder.
- `--service-account-id` is the ID of the sa-kuma service account.

3. Assign the kms.keys.encrypterDecrypter role to the kuma-kms encryption key:

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

Where:

- `--role` is the assigned role.
- `--id` is the ID of the kuma-kms KMS key.
- `--service-account-id` is the ID of the sa-kuma service account.

To assign the storage.viewer and kms.keys.encrypterDecrypter roles to the sa-kuma-bucket service account:

1. In the CLI, assign the storage.viewer role to the folder:

```
yc resource-manager folder add-access-binding \
--id <directory_id> \
--role storage.viewer \
--service-account-id <service_account_id>
```

Where:

- `--id` is the ID of the 'example-folder' folder.
- `--role` is the assigned role.
- `--service-account-id` is the ID of the sa-kuma-bucket service account.

2. Assign the kms.keys.encrypterDecrypter role to the kuma-kms encryption key:

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

Where:

- `--role` is the assigned role.
- `--id` is the ID of the kuma-kms KMS key.
- `--service-account-id` is the ID of the sa-kuma-bucket service account.

8. Creating an audit trail

To create an audit trail:

1. In the management console, go to the **example-folder** folder.
2. Select the **Audit Trails** service.
3. Click **Create trail** and specify a name for the trail you are creating, for example, **kuma-trail**.
4. In the **Destination** section, specify the parameters of the destination object:
   - **Destination**: **Object Storage**.
   - **Bucket**: The name of the bucket, for example **kumabucket**.
   - **Object prefix**: Optional parameter used in the full name of the audit log file.

     Use a prefix if you store audit logs and third-party data in the same bucket. Do not use the same prefix for logs and other objects in the bucket because this may cause logs and third-party objects to overwrite each other.
   - **Encryption key**: specify the kuma-kms encryption key that the bucket is encrypted with.
5. In the **Service account** section, select **sa-kuma**.
6. In the **Collecting management events** section, specify the settings for collecting management events audit logs:
   - **Collecting events**: select **Enabled**.
   - **Resource**: select **Folder**.
   - **Folder**: does not require filling, contains the name of the current folder.
7. In the **Collecting data events**, in the **Collecting events** field, select **Disabled**.
8. Click **Create**.

2 Configuring export of Yandex Cloud events

The bucket must be mounted on the server on which the KUMA collector will be installed.

1. On the server, create a directory for the 'kuma' user:

```
sudo mkdir /home/kuma
```

2. On the server, create a file with a static access key for the sa-kuma-bucket service account and grant appropriate access permissions to the 'kuma' user:

```
sudo bash -c 'echo <access_key_ID>:<secret_access_key> > /home/kuma/.passwd-s3fs'
sudo chmod 600 /home/kuma/.passwd-s3fs
sudo chown -R kuma:kuma /home/kuma
```

3. Install the s3fs package:

```
sudo apt install s3fs
```

4. Create a directory in which you want to mount the bucket and grant permissions to the kuma user:

```
sudo mkdir /var/log/yandex-cloud/
sudo chown kuma:kuma /var/log/yandex-cloud/
```

5. Mount the bucket:

```
sudo s3fs kumabucket /var/log/yandex-cloud -o passwd_file=/home/kuma/.passwd-s3fs -o
url=https://storage.yandexcloud.net -o use_path_request_style -o uid=$(id -u kuma) -o gid=$(id -g kuma)
```

You can configure the bucket to be mounted at operating system startup by adding a line to /etc/fstab, for example:

```
s3fs#kumabucket /var/log/yandex-cloud fuse _netdev,uid=<kuma_uid>,gid=
<kuma_gid>,use_path_request_style,url=https://storage.yandexcloud.net,passwd_file=/home/kuma/.passwd-s3fs 0 0
```

Where:

- `<kuma_uid>` is the ID of the KUMA user in the operating system.
- `<kuma_gid>` is the ID of the KUMA group in the operating system.

To find out the `kuma_uid` and `kuma_gid`, run the following command:

```
id kuma
```

6. Verify that the bucket is mounted:

```
sudo ls /var/log/yandex-cloud/
```

If everything is configured correctly, the command returns `<audit_trail_id>`, where `<audit_trail_id>` is the audit trail ID.

Export of Yandex Cloud events is configured. Events are located in directories in .json files:

```
/var/log/yandex-cloud/{audit_trail_id}/{year}/{month}/{day}/*.json
```

3 Configuring a KUMA collector for receiving and processing Yandex Cloud events

To receive Yandex Cloud events, perform the following actions while creating a KUMA collector:

1. In the KUMA Collector Installation Wizard, at the **Transport** step, select the connector of the **file** type.
2. In the **URL** field, specify the following:

   ```
   /var/log/yandex-cloud/<audit_trail_id>/*/*/*/*.json
   ```

   Where `<audit_trail_id>` is the audit ID.
3. At the **Event parsing** step, in the **Normalizer** field, select **[OOTB] Yandex Cloud**.

4 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Yandex Cloud events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

5 Verifying receipt of Yandex Cloud events by the KUMA collector

To verify whether the Yandex Cloud event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

VMware vCenter

You can configure the receipt of VMware vCenter events in the Kaspersky SIEM.

Configuring event receiving consists of the following steps:

1 Configuring the connection to VMware vCenter

1. Connect to the VMware vCenter web interface under a user account with administrator rights.
2. Go to the **Security&Users** section and select **Users**.
3. Create a user account.
4. Go to the **Roles** section and assign the **Read-only: See details of objects role, but not make changes** role to the created account.

   You will use the credentials of this user account in the secret of the collector.

   For details about creating user accounts, refer to the VMware vCenter documentation.

The connection to VMware vCenter for receiving events is configured.

2 Creating a KUMA collector for receiving VMware vCenter events

To receive VMware vCenter events, while creating the collector, select the **vmware** connector type at the **Transport** step and set mandatory parameters:

- The URL at which the VMware API is available, for example, `https://vmware-server.com:6440`.
- VMware credentials—a secret that specifies the username and password for connecting to the VMware API.

At the **Event parsing** step, select the **[OOTB] VMware vCenter API** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect VMware vCenter events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of VMware vCenter events by the KUMA collector

To verify whether the VMware vCenter event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Veeam Backup & Replication

Kaspersky SIEM enables monitoring of events from Veeam Backup & Replication system (version 12.1) that are received via the syslog protocol.

Configuring the receipt of Veeam Backup & Replication events involves the following steps:

1 Configuring the export of Veeam Backup & Replication events

Event export must be configured using an account with administrator rights.

1. In the Veeam Backup & Replication web interface, open the **Options** → **Event forwarding** section.
2. In the **Syslog servers** section, click **Add**.
3. In the **Server** field, specify the fully qualified domain name (FQDN) or IPv4 address of the KUMA collector server. You cannot specify an IPv6 address in this field.
4. In the **Port** field, specify the port that the KUMA collector is listening on.

By default, the Veeam Backup & Replication system sends events to the following ports, depending on the protocol used:

- 514 for TCP and UDP
- 6514 for TLS

5. In the **Transport** drop-down list, select a protocol: **TCP**, **UDP**, or **TLS**.
6. Click **OK**.

Transferring of events from Veeam Backup & Replication to the KUMA collector is configured.

2 Creating a KUMA collector for receiving Veeam Backup & Replication events

When creating a collector in the Kaspersky SIEM web interface, at the **Transport step**, you need to specify the type of connector that is used when configuring event export. To receive Veeam Backup & Replication events, at the **Event parsing** step, select the **[OOTB] Veeam Software Veeam Backup & Replication syslog** normalizer.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector for collecting Veeam Backup & Replication events, install the KUMA collector on the server of a network infrastructure intended for receiving events.

4 Verifying receipt of Veeam Backup & Replication events by the KUMA collector

To verify whether receipt of events from Veeam Backup & Replication is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Mail and collaboration systems

This section describes how to configure the receiving of events from mail servers and collaboration platforms.

CommuniGate Pro

You can configure the receipt of CommuniGate Pro 6.1 and 6.5.1 events in Kaspersky SIEM. Integration is only possible when sending events via syslog using the TCP protocol. Processing of some SIP module events is supported (such events contain the "SIPDATA" character sequence).

The CommuniGate Pro system generates an audit event as several separate records that look like this:

```
<event code> timestamp ID direction: information from base event 1
```

```
<event code> timestamp ID direction: information from base event 2

<event code> timestamp ID direction: base information n
```

A set of KUMA resources is used to process CommuniGate Pro events; this resource set must be applied when creating a collector:

- Normalizer
- Aggregation rule
- Filters for destinations

The collector aggregates multi-line base events based on event ID, normalizes them, and sends the aggregated event to the storage and the correlator.

The aggregated event has the following form:

```
Service information from the aggregation rule: ID: information from base event 1,
information from base event 2, information from base event n
```

After aggregation, the received event is sent to the same collector where the aggregated event is normalized.

Processing algorithm for CommuniGate Pro events

The following algorithm was implemented to process CommuniGate Pro events:

1. Initial normalization

   At this stage, the initial normalization of base events is performed. The first character in the base event is a numeral. The events are brought to a format suitable for subsequent aggregation: the first character is extracted from the event and put into the DeviceCustomString1 field, the identifier is put into the ExternalID field, and the host name is put into the DeviceHostName field. Basic normalization is performed in the main normalizer.

2. Checking for aggregation

   The event is examined to see if it is aggregated or not. As a result, non-aggregated events (the first character is a numeral) have an aggregation rule applied, and then aggregated events are sent to re-normalization. Aggregation is performed using the **[OOTB] CommuniGate Pro. Aggregation rule**.

3. Applying the aggregation rule

   At this stage, the aggregation rule is applied to the events, the base events are collated and take the following form:

   Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

   After aggregation, the collated event is sent back to the same collector to subject the aggregated event to normalization.

   To close the event processing loop, you must specify the same collector as the destination. In the diagram, the destination is named "Loop" to draw attention to the event processing loop. You can give an arbitrary name to your destination.

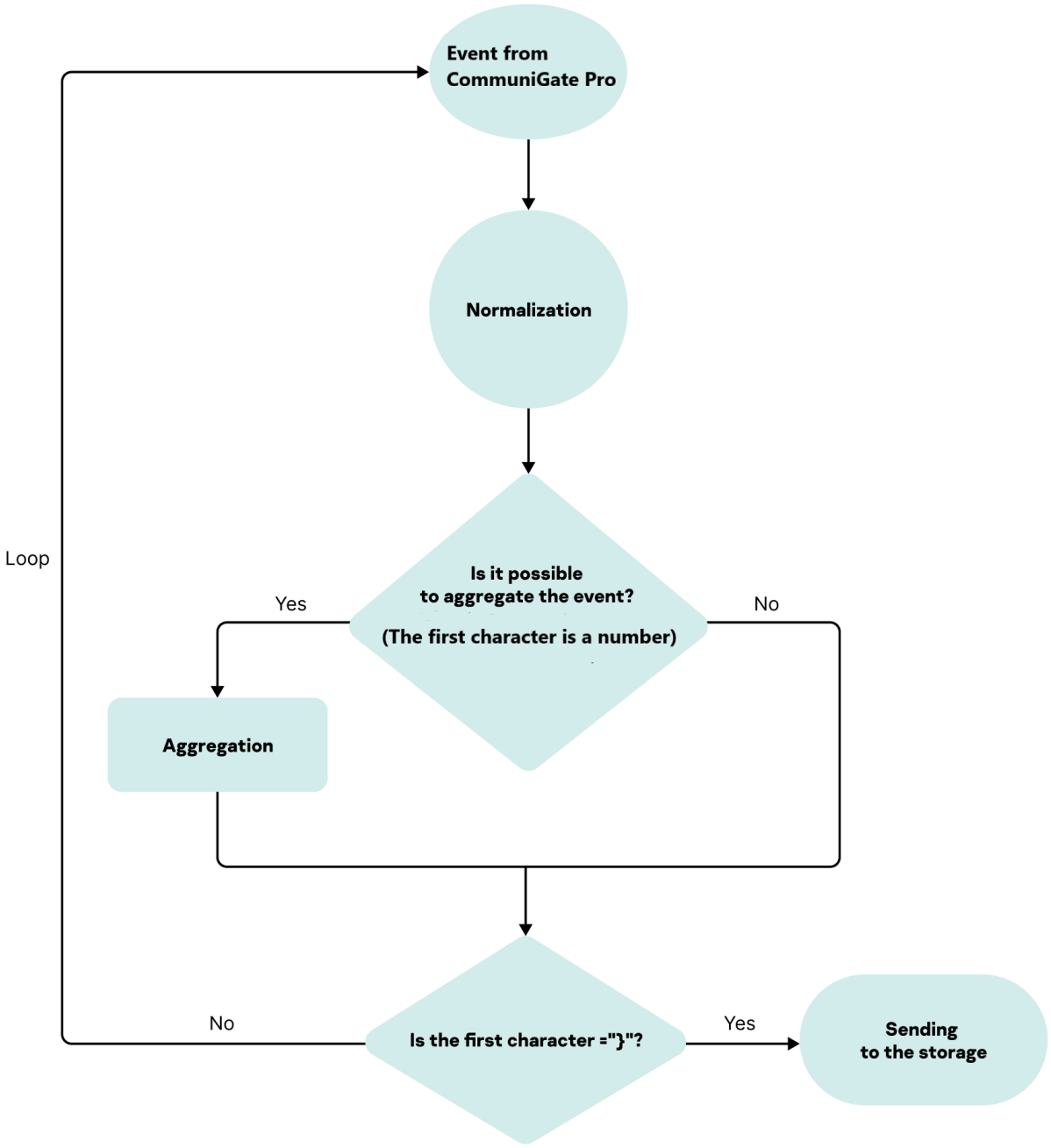
4. Normalization of the aggregated event

   Normalization of the aggregated event that begins with a "{" character is performed in the following extra normalizers: Aggregated events, Aggregated events - kv part.

5. Sending to storage and the correlator

   Aggregated and normalized events are sent to storage and the correlator.

The following figure shows the flow chart of CommuniGate Pro event processing.



Processing diagram for events from the CommuniGate Pro system

Configuring event receiving consists of the following steps:

1 Configuring CommuniGate Pro to send events

By default, CommuniGate Pro audit events are sent to .log files in the `/var/CommuniGate/SystemLogs/` directory.

To send events to Kaspersky SIEM, you need to install the KUMA agent on the CommuniGate Pro server and configure it to read .log files in the `/var/CommuniGate/SystemLogs/` directory and send them to the KUMA collector over TCP.

1. In the web interface, go to **Resources and services** → **Agents** and click **Add**.

2. This opens the **Create agent** window; in that window, on the **Basic settings** tab, in the **Name** field, specify the agent name.

3. Go to the **Connection No. 1** tab.

4. In the **Connector** group of settings on the **Basic settings** tab, set the following values for the connector:

   a. In the **Name** field, enter a name, for example, `CommuniGate file`.

   b. In the **Type** drop-down list, select **file**.

   c. In the **File path** field, enter the following value:

   ```
   /var/CommuniGate/SystemLogs/.*.log
   ```

5. In the **Destinations** group of settings on the **Basic settings** tab, set the following values for the destination:

   a. In the **Name** field, enter a name, for example, `CommuniGate TCP collector`.

   b. In the **Type** drop-down list, select **tcp**.

   c. In the **URL** field, enter the FQDN or IP address and port of the KUMA collector.

6. Then click the **Create** button.

When the agent service will be created in Kaspersky SIEM, install the agent on the network infrastructure devices from which you want to send data to the collector.

2 Creating a KUMA collector for receiving CommuniGate Pro events

1. Import the [OOTB] CommuniGate Pro package from the KUMA repository. The package is available for KUMA 3.0 and newer versions.

2. Create a new collector, and in the Collector Installation Wizard, configure the following:

   a. At the **Transport** step, in the **Type** field, select the **tcp** type, and in the **URL** field, specify the FQDN or IP address and port of the collector.

   b. At the **Event parsing** step, click **Add event parsing**, and in the displayed **Basic event parsing** window, in the **Normalizer** drop-down list, select the **[OOTB] CommuniGate Pro** normalizer.

   c. At the **Event aggregation** step, click **Add aggregation rule**, and in the displayed **Event aggregation** window, in the **Aggregation rule** drop-down list, select **[OOTB] CommuniGate Pro. Aggregation rule**.

d. At the **Routing** step, click **Add** and in the displayed **Create destination** window, create three destination points one by one—the same collector with the name `Loop`, a storage, and a correlator:

1. Create a destination named `Loop` with the following parameters.

   - On the **Basic settings** tab, in the **Type** drop-down list, select the **tcp** transport type; in the **URL** field, specify the FQDN or IP address and port of the collector that you specified before at step 2.1 of these instructions.

   - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **[OOTB] CommuniGate Pro. Filter for event aggregation** filter.

   This configuration is necessary to send the aggregated event to the same collector for subsequent normalization.

2. Create a correlator destination:

   - On the **Basic settings** tab, in the **Type** drop-down list, select **correlator** and fill in the **URL** field.

   - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

3. Create a storage destination:

   - On the **Basic settings** tab, in the **Type** drop-down list, select **storage** and fill in the **URL** field.

   - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

   This configuration is necessary to send the aggregated normalized event to storage and the correlator.

3. Click the **Create** button.

   The collector service with the specified settings is created. The command for installing the service on the server is displayed.

4. Copy the command for installing the KUMA collector.

❸ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect CommuniGate Pro events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❹ Verifying receipt of CommuniGate Pro events by the KUMA collector

To verify whether the CommuniGate Pro event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Postfix

You can configure the receipt of Postfix events in KUMA. Integration is only possible when sending events via syslog using the TCP protocol. The resources described in this article are available for KUMA 3.0 and newer versions.

The Postfix system generates events in two formats:

- Multi-line events containing information about messages (with a unique ID). These events have the following form:

  `<syslog PRI> time host process_name: ID: information from base event 1`

  `<syslog PRI> time host process_name: id: info from base event 2`

- Single-line events containing information about errors (without an ID). These events have the following form:

  `<syslog PRI> time host process_name: severity: basic information for parsing`

A set of KUMA resources is used to process Postfix events; this resource set must be applied when creating a collector:

- Normalizer
- Aggregation rule
- Filters for destinations

The collector aggregates multi-line base events based on event ID, normalizes them, and sends the aggregated event to the storage and the correlator.

The aggregated event has the following form:

Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

After aggregation, the received event is sent to the same collector where the aggregated event is normalized.

Processing algorithm for Postfix events

The following algorithm was implemented to process Postfix events:

1. Initial normalization

   At this stage, initial normalization is performed for base events received via syslog that begin with the "<" character. The events are brought to a format suitable for subsequent aggregation: the first character is extracted from the event and put into the FlexString1 field, the identifier is put into the ExternalID field, and the host name is put into the DeviceHostName field. Basic normalization is performed in the main normalizer.

2. Checking for aggregation

   The event is examined to see if it is aggregated or not. As a result, non-aggregated events (the first character is not "{" and the ID is not empty) have an aggregation rule applied, and then aggregated events are sent for re-normalization.

3. Applying the aggregation rule

At this stage, the aggregation rule is applied to the events, the base events are collated and take the following form:

Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

4. After aggregation, the collated event is sent back to the same collector to subject the aggregated event to normalization.

   To close the event processing loop, you must specify the same collector as the destination. In the diagram, the destination is named "Loop" to draw attention to the event processing loop. You can give an arbitrary name to your destination.

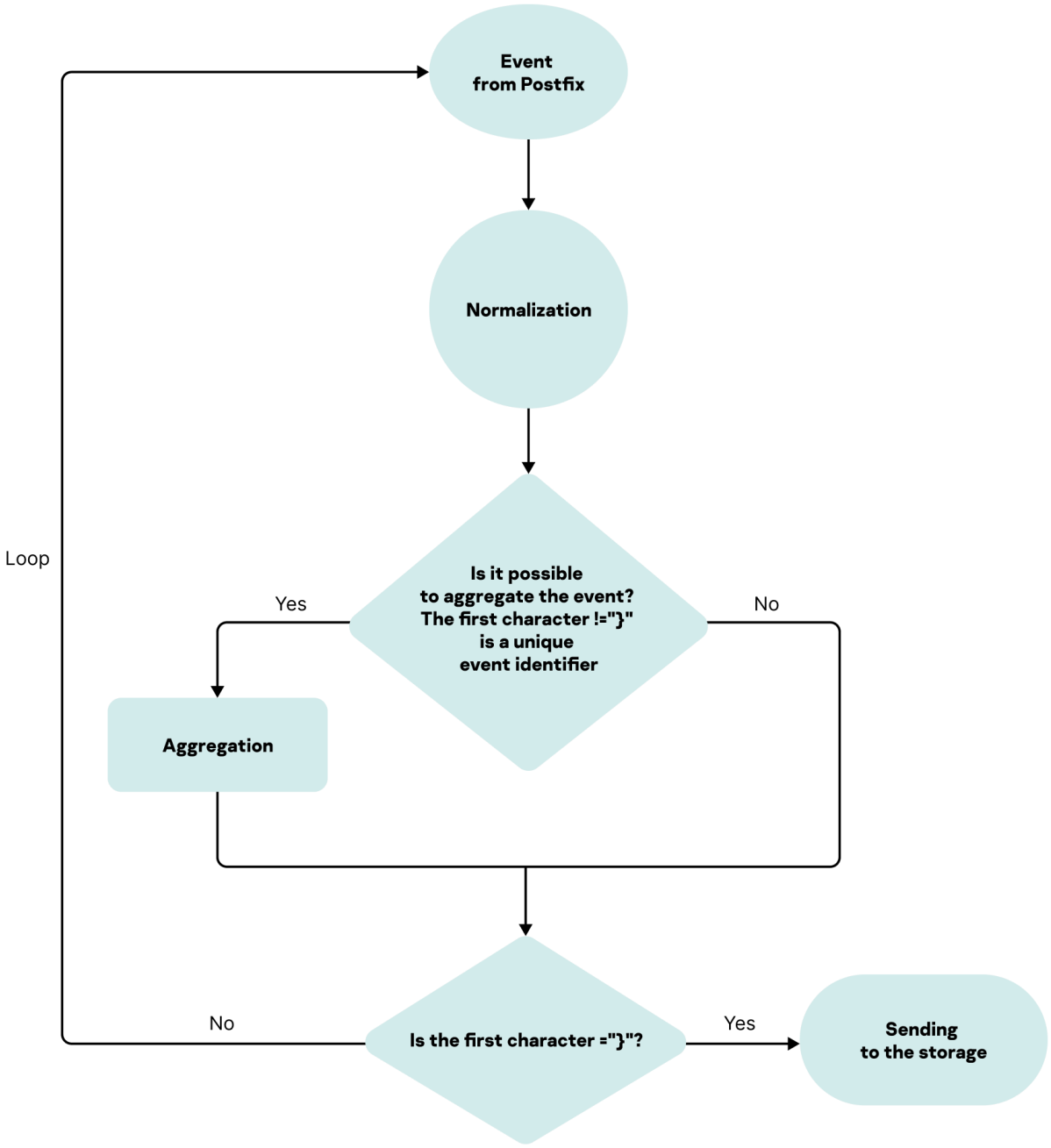
5. Normalization of the aggregated event

   Normalization of the aggregated event that begins with a "{" character is performed in the following extra normalizers: Aggregated events, Aggregated events. Message KV parser, Aggregated events. Message regex 1, Aggregated events. Message regex 2.

6. Sending to storage and the correlator

   Aggregated and normalized events are sent to storage and the correlator.

The following figure shows the flow chart of Postfix event processing.



Processing diagram for events from the Postfix system

Configuring event receiving consists of the following steps:

1 Configuring Postfix to send events

By default, audit events of the Postfix system are logged to `/var/log/maillog` or `/var/log/mail`.

1. Create a backup copy of the `/etc/rsyslog.conf` file.
2. Open the `/etc/rsyslog.conf` file for editing.

3. Add the following line to the end of the `/etc/rsyslog.conf` file:

```
mail.* @@<IP address of the KUMA collector>:<port of the KUMA collector>
```

4. Save the `/etc/rsyslog.conf` file.

5. Restart the rsyslog service:

```
sudo systemctl restart rsyslog
```

2 Creating a KUMA collector for receiving Postfix events

1. Import the [OOTB] Postfix package from the KUMA repository.

2. Create a new collector, and in the Collector Installation Wizard, configure the following:

   a. At the **Transport** step, in the **Type** field, select the **tcp** type, and in the **URL** field, specify the FQDN or IP address and port of the collector.

   b. At the **Event parsing** step, click **Add event parsing**, and in the displayed **Basic event parsing** window, in the **Normalizer** drop-down list, select the **[OOTB] Postfix syslog** normalizer.

   c. At the **Event aggregation** step, click **Add aggregation** rule, and in the displayed **Event aggregation** window, in the **Aggregation rule** drop-down list, select **[OOTB] Postfix. Aggregation rule**.

   d. At the **Routing** step, click **Add** and in the displayed **Create destination** window, create three destination points one by one—the same collector with the name `Loop`, a storage, and a correlator.

      1. Create a destination named `Loop` with the following parameters.

         - On the **Basic settings** tab, in the Type drop-down list, select the **tcp** transport type; in the **URL** field, specify the FQDN or IP address and port of the collector that you specified before at step 2.1 of these instructions.

         - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **Postfix. Filter for event aggregation** filter.

         This configuration is necessary to send the aggregated event to the same collector for subsequent normalization.

      2. Create a correlator destination:

         - On the **Basic settings** tab, in the **Type** drop-down list, select **correlator** and fill in the **URL** field.

         - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **Postfix. Aggregated events to storage and correlator**.

3. Create a storage destination:

   - On the **Basic settings** tab, in the **Type** drop-down list, select **storage** and fill in the **URL** field.
   - On the **Advanced settings** tab, in the **Filter** drop-down list, select the **Postfix. Aggregated events to storage and correlator**.

   This configuration is necessary to send the aggregated normalized event to storage and the correlator.

3. Click the **Create** button.

   The collector service is created with the settings specified in the KUMA web interface. The command for installing the service on the server is displayed.

4. Copy the command for installing the KUMA collector.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Postfix events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Postfix events by the KUMA collector

To verify whether the Postfix event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Sendmail

Follow these steps to configure receipt of events from the Sendmail Kaspersky SIEM agent:

1 Configuring Sendmail logging

By default, events of the Sendmail system are logged to syslog.

To make sure that logging is configured correctly:

1. Connect via SSH to the server on which the Sendmail system is installed.

2. Run the following command:

   ```
   cat /etc/rsyslog.d/50-default.conf
   ```

   The command should return the following string:

   ```
   mail.*                          -/var/log/mail.log
   ```

If logging is configured correctly, you can proceed to configuring the export of Sendmail events.

2 Configuring the event source server

Events are sent from the Sendmail mail agent server to the Kaspersky SIEM collector using the rsyslog service.

To configure transmission of Sendmail events to the collector:

1. Connect to the server where Sendmail is installed using an account with administrator rights.
2. In the `/etc/rsyslog.d` directory, create the `Sendmail-to-siem.conf` file and add the following line to it:

   ```
   If $programname contains 'sendmail' then @<collector_IP>:<collector_port>
   ```

   Example

   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   If you want to send events via TCP, the contents of the file must be as follows:

   ```
   If $programname contains 'sendmail' then @@<collector IP>:<collector_port>
   ```

   where:

   - `<collector_IP>` is the collector IP address.
   - `<collector_port>` is the collector port.
3. Create a backup copy of the `/etc/rsyslog.conf` file.
4. Add the following lines to the `/etc/rsyslog.conf` configuration file:

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Save your changes.
6. Restart the rsyslog service by executing the following command:

   ```
   sudo systemctl restart rsyslog.service
   ```

3 Creating a KUMA collector

When creating a collector in the Kaspersky SIEM web interface, at the **Event parsing** step, select the **[OOTB] Sendmail syslog** normalizer, and at the **Transport** step, select the **tcp** or **udp** connector type.

4 Installing the KUMA collector.

Once you have created and configured the collector to collect Sendmail events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

5 Verifying receipt of Sendmail events in the KUMA collector

To verify that the Sendmail event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

VK WorkSpace Mail

KUMA enables monitoring of events from VK WorkSpace Mail 1.23 that are sent to the Kaspersky SIEM in the syslog format.

Configuring event receiving consists of the following steps:

1 Configuring transmission of VK WorkSpace Mail events

To configure the transfer of the events from VK WorkSpace Mail to KUMA:

1. In the VK WorkSpace Mail web interface, go to the **Settings for duplicating user actions to external storage**.
2. Select the **Duplicate user actions to syslog** check box.
3. In the **Syslog server address** field, enter the IP address or FQDN of the KUMA collector.
4. In the **Syslog server port** field, specify the port that the KUMA collector is listening on.
5. In **Syslog protocol, TCP or UDP** field, select the communication protocol.
6. In the **Syslog data ID** field, specify `bein`.

2 Creating a KUMA collector for receiving VK WorkSpace Mail events

To receive VK WorkSpace Mail audit events, while creating the collector, select the **[OOTB] VK WorkSpace Mail syslog** normalizer at the **Event parsing** step. Also, on the **Transport** tab, specify the same port and protocol of the syslog server that you specified when configuring the transfer of VK WorkSpace Mail events.

3 Installing a collector in the network infrastructure

Once you have created and configured the collector to collect VK WorkSpace Mail events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of VK WorkSpace Mail events by the KUMA collector

To verify whether the VK WorkSpace Mai event source server is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Other specialized systems

This section describes how to configure the receiving of events from specialized solutions.

Codemaster Mirada

You can configure the receipt of Codemaster Mirada events in the Kaspersky SIEM (KUMA).

Configuring event receiving consists of the following steps:

1 Configuring audit of the Codemaster Mirada system

The Codemaster Mirada system can send events over the Syslog protocol.

1. Connect to the Codemaster Mirada web interface under a user account with administrator rights.
2. Go to the **Settings** → **Syslog** section.
3. Enable the event transmission service using the toggle switch.
4. Select the type and format of the protocol by clicking the dot-in-a-circle icon.
5. In the **Host** field, specify the IP address of the KUMA collector.
6. In the **Protocol** field, specify the **UDP** or **TCP** transport protocol.
7. In the **Port** field, specify the port that the KUMA collector is listening on.
   The default port is 514.
8. In the **Format** field, specify the **RFC 3164** standard.
9. Click **Save** in the lower part of the page to save the changes.

2 Creating a KUMA collector for receiving Codemaster Mirada events

To receive Codemaster Mirada events, while creating the collector, select the **[OOTB] Codemaster Mirada syslog** normalizer at the **Event parsing** step, and select the **tcp** or **udp** connector type at the **Transport** step.

3 Installing a collector in the network infrastructure

Once you configured the collector for receiving Codemaster Mirada events, install the KUMA collector on the server of the network infrastructure intended for receiving events.

4 Verifying receipt of Codemaster Mirada events by the KUMA collector

To verify whether the Codemaster Mirada event source server is configured correctly, you can search for related events in the Kaspersky SIEM (KUMA) web interface.

APKSh Kontinent

The Kaspersky SIEM distribution kit includes the kuma-kont utility, which consists of an executable file and a configuration file. This utility allows lets you connect to the MSSQL database, receive events of the Kontinent encryption system, and send data to the KUMA collector in JSON format. Data import is supported for Kontinent 3.9.2.

The list of operating systems that support the kuma-kont utility is given in the Software requirements section.

Configuring the retrieval of Kontinent events from an MSSQL database and sending them to the KUMA collector involves the following steps:

1 Creating a KUMA collector for receiving Kontinent 3.9 events

When creating a collector at the **Event parsing** step, select the **[OOTB] SecurityCode Continent 3.9 json** normalizer. In the **Transport** tab, you need to specify the port and protocol that are specified in the kuma-kont-config.yaml configuration file in the "KUMA Collector" group of settings.

2 Installing a collector in the network infrastructure

Once you have created and configured the collector to collect Kontinent events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

3 Creating a user account in an MS SQL DBMS

Create an account in the database with the minimum necessary rights to connect and read data from the following tables: ALERTLOG, SERVERACCESSLOG, SYSTEMLOG, PACKETLOG, FILTERS.

4 Ensuring network connectivity

You must ensure network connectivity between the server on which the utility is running and the database server of the Kontinent system, as well as between the server on which the utility is running and the KUMA collector server.

5 Creating the kuma-kont-config.yaml configuration file

1. Go to the KUMA installer directory by executing the following command:

```
cd kuma-ansible-installer/roles/kuma/files
```

2. Extract the kuma-kont.tar archive:

```
tar -xvf kuma-kont.tar
```

3. Go to the directory of the utility:

```
cd kuma-kont
```

4. Copy the kuma-kont-config-template.yaml template to create a configuration file named kuma-kont-config.yaml:

```
cp kuma-kont-config-template.yaml kuma-kont-config.yaml
```

5. Change read permissions for the configuration file:

```
sudo chown <user account>:<user account> kuma-kont-config.yaml
sudo chmod 600 kuma-kont-config.yaml
```

   Replace `<user account>` with the user name of the operating system user that the service will use.

6. Edit the settings in the `kuma-kont-config.yaml` configuration file.

   Settings in the kuma-kont-config.yaml configuration file

   The table lists the settings that you can specify in the kuma-kont-config.yaml file.

Settings in the kuma-kont-config.yaml configuration file

Setting	Description
`debug`	Optional setting in the **General settings** group. Used when debug level log output is required. If false, only start and stop messages are included, as well as errors that occurred during the sending process. Available values: • **true** • **false** The default value is **false**.
`need_reconnect`	An optional setting in the **General settings** group. This setting determines whether the utility reconnects to the database to make each request. Available values: • **true** • **false** The default value is **false**.
`state_file`	Required setting in the **General settings** group. Absolute path to the JSON file in which the state of the processed logs is saved. The file is created automatically at this path. Make sure the user has sufficient permissions to write to this directory. Example: /home/user/kuma-kont/state.json
`log_file_path`	Required setting in the **General settings** group. Absolute path to the log file for recording connector activity. The file is created automatically at this path. Make sure the user has sufficient permissions to write to this directory. Example: /home/user/kuma-kont/kuma-kont.log
`poll_interval`	An optional setting in the **General settings** group. Database polling interval. The default value is 10 seconds. For high EPS, we recommend a value less than 15 seconds.
`name`	Required setting in the **Kontinent Database** group. Name of the database in which Kontinent logs are received.
`user`	Required setting in the **Kontinent Database** group. Name of the database user.
`password`	Required setting in the **Kontinent Database** group. Password of the database user.
`host`	Required setting in the **Kontinent Database** group. URL of the database server.
`port`	Required setting in the **Kontinent Database** group. Port of the database server. Make sure it is accessible from the server where the utility is installed.
`limit`	Optional setting in the **Kontinent Database** group. Limit on the number of events that can be downloaded from the database as part of one poll. By default, 100,000 events per database poll. If EPS is high, we recommend a value equal or greater than this.
`alert_log`	Optional setting in the **Last Id** group. Specifies the event of the AlertLog type from which you want to start sending events to the KUMA collector. Only works on first run or when the state file does not exit. The default value is 0.
`packet_log`	Optional setting in the **Last Id** group. Specifies the event of the PacketLog type from which you want to start sending events to the KUMA collector. Only works on first run or when the state file does not exit. The default value is 0.

Setting	Description
`server_access_log`	Optional setting in the **Last Id** group. Specifies the event of the ServerAccessLog type from which you want to start sending events to the KUMA collector. Only works on first run or when the state file does not exit. The default value is 0.
`system_log`	Optional setting in the **Last Id** group. Specifies the event of the SystemLog type from which you want to start sending events to the KUMA collector. Only works on first run or when the state file does not exit. The default value is 0.
`address`	Required setting in the **KUMA Collector** group. Fully qualified domain name (FQDN) or IP address of the server where the KUMA collector is installed.
`port`	Required setting in the **KUMA Collector** group. Port of the KUMA collector.
`protocol`	Required setting in the **KUMA Collector** group. Data transfer protocol used by the KUMA collector. If the udp protocol is used, events are not resent if connection to the KUMA collector is lost. Available values: • **tcp** • **udp**

Specify the values of the following settings:

- General settings: `state_file`, `log_file_path`.
- Kontinent Database: `name`, `user`, `password`, `host`, port.
- KUMA Collector: `address`, `port`, `protocol`.

7. Save the changes to the file.

The configuration file will be created.

6 Creating a kuma-kont service

1. Change the execution permissions for the executable file:

```
sudo chown <user account>:<user account> <path to an executable file>
sudo chmod 700 <path to an executable file>
```

2. Create the `kuma-kont.service` file in the `/etc/systemd/system/` directory with the following contents:

```
[Unit]
Description=Connector Kontinent 3.9
After=network.target
[Service]
User=<account>
ExecStart=<path to an executable file> --config <path to a configuration file>
Restart=always
RestartSec=10
[Install]
WantedBy=multi-user.target
```

   Replace `<user account>` with the user name of the operating system user that the service will use.

3. Specify the path to the `kuma-kont` executable file in the `ExecStart` field.

   For example, if the `kuma-kont` file is located in the `/usr/bin/` directory, leave the default value.

4. Specify the path to the `kuma-kont-config.yaml` configuration file in the `ExecStart` field.

   For example, if the `kuma-kont-config.yaml` file is located in the `/path/to/` directory, specify that path.

   Example kuma-kont.service file

```
[Unit]
Description=Continent Service
After=network.target
[Service]
User=user-example
ExecStart=./usr/bin/kuma-kont --config /path/to/kuma-kont-config.yaml
Restart=always
RestartSec=10
[Install]
WantedBy=multi-user.target
```

5. Load the systemd configuration:

```
sudo systemctl daemon-reload
```

6. Make the service run at startup:

```
sudo systemctl enable kuma-kont
```

   The kuma-kont utility will be started as a service at system startup.

7 Starting the kuma-kont utility

After activation, the utility starts exporting events from the MS SQL database and sending them to the KUMA collector. It keeps a log in the kuma-kont.log file.

To start the utility service, run the following command:

```
sudo systemctl start kuma-kont
```

The collection of events from the MSSQL database begins and the events are sent to the KUMA collector.

The utility service can be controlled using the following commands:

```
To start the kuma-kont service
sudo systemctl start kuma-kont
```

```
To stop the kuma-kont service
sudo systemctl stop kuma-kont
```

```
To restart the kuma-kont service
sudo systemctl restart kuma-kont
```

You can also send events using the kuma-kont utility running as an application. To start sending events to the KUMA collector, run the following command while in the directory with the executable file:

```
./kuma-kont --config <path to the kuma-kont-config.yaml file>
```

Behavior when connection is lost

Connection to the MSSQL database.

If the connection to the MS SQL database is lost, the utility tries to reconnect to it every **n** seconds (where **n** is equal to the value of the `poll_interval` option in the configuration file) until the connection is restored.

Connection to the KUMA collector

If the TCP protocol is used to send events, when the connection to the KUMA collector is lost, the utility also attempts to restore it. The interval between connection attempts increases until it reaches one hour, and subsequent reconnection attempts are made once per hour.

Known limitations

The event from the `AlertLog` table with the `AL_CATEGORY=5` value is not fully decoded.

Ansible

Configuring the receipt of events from the Ansible system (version 2.10.8) received via the Syslog protocol in Kaspersky SIEM consists of the following steps:

1 Configuring the export of Ansible events to KUMA

1. Make sure that the rsyslog service is installed on the event source server. To do this, run the following command under an account with administrator rights:

   ```
   sudo systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. In the `/var/log/` directory, create the `ansible` directory.

3. Create the `ansible.log` file in the `/var/log/ansible` directory.

4. Switch to your Ansible working directory.

   Example

   ```
   cd ~/ansible-playbooks/
   ```

5. Create or edit an Ansible configuration file:

   ```
   sudo nano ansible.cfg
   ```

   The `ansible.cfg` file should look like this:

   ```
   [defaults]
   log_path = /var/log/ansible/ansible.log
   log_level = INFO
   inventory = <inventory file or path to the inventory file>
   ```

6. Go to the `/etc/rsyslog.d/` directory and create an `ansible-to-siem.conf` file.

7. Add the following lines to the `/etc/rsyslog.d/ansible-to-siem.conf` configuration file:

```
module(load="imfile")

input(type="imfile"
    File="/var/log/ansible/ansible.log"
    Tag="tag_Ansible_log:"
    facility="local1"
    Startmsg.regex="^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}"
)

template(name="Ansible_log" type="string"
    string="<%pri%>%timegenerated% %HOSTNAME% %syslogtag% %msg%\n"
)

if $syslogtag startswith 'tag_Ansible_log:' then {
    action(type="omfwd"
           target="<IP address of the KUMA collector>"
           port="<port of the KUMA collector>"
           protocol="<udp or tcp>"
           template="Ansible_log")
stop
}
```

If the value of the `facility local1` parameter is already in use by another application on the server, change the value of the `facility` parameter for Ansible to a different value.

8. Save the changes to the `/etc/rsyslog.d/ansible-to-siem.conf` configuration file.

9. Add the following lines to the `/etc/rsyslog.conf` configuration file:

```
$IncludeConfig /etc/rsyslog.d/ansible-to-siem.conf
$RepeatedMsgReduction off
```

10. Save changes to the `/etc/rsyslog.conf` configuration file.

11. Restart the rsyslog service:

```
sudo systemctl restart rsyslog.service
```

Ansible does not perform log rotation. To reduce the risk of disk space filling up, we recommend using an external log rotation tool such as Logrotate or Logadm.

❷ Creating a KUMA collector for receiving Ansible events

When creating a collector in KUMA, at the **Event parsing** step, select the **[OOTB] Ansible syslog** normalizer.

❸ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Ansible events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Ansible events by the KUMA collector

To verify whether receipt of events from Ansible is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Grafana

Configuring the receiving of audit events from the Grafana system (version 9.5.15) in Kaspersky SIEM involves the following steps:

1 Configuring audit and sending Grafana events to KUMA

1. Open the configuration file `/etc/grafana/grafana.ini` and change the values of the following parameters:

```
mode = syslog
     level = info
```

2. Change the values of the following parameters depending on the protocol used:

```
To send events over UDP

level = info
format = json
network = udp
address = "<IP address of the KUMA collector>:<port of the KUMA collector>"
tag = Grafana
```

```
To send events over TCP

level = info
format = json
network = tcp
address = "<IP address of the KUMA collector>:<port of the KUMA collector>"
tag = Grafana
```

3. Restart Grafana service:

```
systemctl restart grafana-server
```

2 Creating a KUMA collector for receiving Grafana events

When creating a collector in Kaspersky SIEM, at the **Transport** step, specify the same port and protocol that you configured for sending Grafana events. To receive events from Grafana, select the **[OOTB] Grafana json** normalizer at the **Event parsing** step.

3 Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect Grafana events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4 Verifying receipt of Grafana events by the KUMA collector

To verify whether receipt of events from Grafana is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

TeamPass

> Before configuring, make sure that the TeamPass database tables use the prefix **teampass_**. If the prefix is different, you must change the table names in the queries of the **[OOTB] TeamPass MySQL** connector to match the name used in your instance.

Configuring the receipt of TeamPass system events (version 3.1) from the MySQL database in Kaspersky SIEM involves the following steps:

1 Creating an account in MySQL

Event submission must be configured under an account with the minimum required permissions to connect to the database and read data from tables.

1. Start a command prompt on the server where MySQL is installed.
2. Log in to the DBMS under the administrator account:

   ```
   mysql --user=root --password=<password> --database=<database name>
   ```

3. Create a user account:

   ```
   CREATE USER <login> IDENTIFIED BY '<password>';
   ```

4. Grant the account read permissions for the database:

   ```
   GRANT SELECT ON <database>.* TO <login>;
   ```

5. Apply the changes:

```
FLUSH PRIVILEGES;
EXIT
```

The user account is created.

6. Check access to the database:

   a. Start a command prompt on the server where MySQL is installed.

   b. Define the port for connecting to the DBMS:

   ```
   mysql --user=root --password=<password> -e "SHOW VARIABLES LIKE 'port';"
   ```

   The default port is 3306.

   c. Run a database query under the new account:

   ```
   mysql -h <server> --user=<login> --password=<password> -P <port> <database name> -e "SELECT ls.id AS id,
   ls.type AS category, ls.date AS date, ls.label AS action, ls.qui AS suser_id, ls.field_1 AS duser_id,
   tu1.login AS suser, tu2.login AS duser FROM teampass_log_system AS ls LEFT JOIN teampass_users tu1 ON
   ls.qui = tu1.id LEFT JOIN teampass_users tu2 ON ls.field_1 = tu2.id ORDER BY ls.id"
   ```

If you have access to the database, the query result appears on the screen.

2 Creating a secret

Once you have created and configured an account in MySQL, you need to add a secret in the Kaspersky SIEM web interface. This resource is used to store credentials for connecting to MySQL.

1. In the web interface, go to **Resources** → **Secrets**.

   The list of available secrets will be displayed.

2. Select the **[OOTB] TeamPass MySQL** secret.

   The secret window is displayed

3. In the **URL** field, specify a string of the following form:

   ```
   mysql://<user>:<password>@tcp(<server>:<port>)/<database>
   ```

   where:

   - `user` is the name of the created MySQL account with rights to connect and work with the database.
   - `password` is the password of the created MySQL account.

- `server` is name or IP address of the server with the MySQL database.
- `database_name` is the name of the TeamPass database.

```
Example

mysql://user:password@tcp(teampass.example.com:3306)/teampass_db
```

If the MS SQL account password contains special characters (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), convert them to URL format.

4. Click **Save**.

For security reasons, the string specified in the URL field is hidden after the secret is saved.

❸ Creating a KUMA collector for receiving **TeamPass** events

When creating a collector in Kaspersky SIEM, at the **Transport** step, select the **[OOTB] TeamPass MySQL** connector. At the **Event parsing** step, select the **[OOTB] TeamPass SQL** normalizer.

❹ Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect TeamPass events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

❺ Verifying receipt of events from **TeamPass** by the KUMA collector

To verify whether receipt of events from TeamPass is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

SaltStack

Configuring the receipt of events from the SaltStack system (version 3004.1) via the Syslog protocol in Kaspersky SIEM involves the following steps:

1 Configuring the export of SaltStack events to KUMA

1. Make sure that the rsyslog service is installed on the event source server. To do this, run the following command under an account with administrator rights:

   ```
   sudo systemctl status rsyslog.service
   ```

   If the rsyslog service is not installed on the server, install it by executing the following commands:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. Go to the `/etc/rsyslog.d/` directory and create a `saltstack-to-siem.conf` file.

3. To send events, add the following lines to the `/etc/rsyslog.d/saltstack-to-siem.conf` configuration file, depending on the protocol used:

   - To send events over UDP:

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @<collector IP address>:<collector port>
     ```

     Example

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @192.168.1.5:1514
     ```

   - To send events over TCP:

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @@<collector IP address>:<collector port>
     ```

     Example

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @@192.168.1.5:1514
     ```

4. Save changes to the `saltstack-to-siem.conf` configuration file.

5. Add the following strings to the `/etc/rsyslog.conf` configuration file:

   ```
   $IncludeConfig /etc/rsyslog.d/saltstack-to-siem.conf
   $RepeatedMsgReduction off
   ```

6. Save changes to the `/etc/rsyslog.conf` configuration file.

7. Restart the rsyslog service:

   ```
   sudo systemctl restart rsyslog.service
   ```

2. Creating a KUMA collector for receiving SaltStack events

When creating a collector in Kaspersky SIEM, at the **Event parsing** step, select the **[OOTB] SaltStack syslog** normalizer.

3. Installing the KUMA collector in the network infrastructure

Once you have created and configured the collector to collect SaltStack events, install the KUMA collector on the server of a network infrastructure intended for reception of events.

4. Verifying receipt of SaltStack events by the KUMA collector

To verify whether receipt of events from SaltStack is configured correctly, you can search for related events in the Kaspersky SIEM web interface.

Monitoring event sources

In an organization, there can be multiple different event sources: domain controllers, Kaspersky Security Center servers, and workstations protected by Kaspersky Endpoint Security. If a source stops sending events to KUMA, it creates an information security risk. You need to watch for the interruption of event stream from sources and send notifications about such situations to system administrators.

To learn more about the event source monitoring, watch this video:

https://www.youtube.com/watch?v=9hC8u_zQq2k

How to configure monitoring of event sources

By default, KUMA determines the event source by the fields `DeviceProduct`, `DeviceHostName`, `DeviceAddress`, `DeviceProcessName`. This data is displayed in the name of the event source. If necessary, you can manually specify the fields by which event sources are identified.

To monitor an event stream from a source (for example, to automatically detect when it becomes too high, too low, or stops altogether), you can apply a *monitoring policy* to the event source. By default, the solution includes three monitoring policies: High bounds policy, Low bounds policy, and Middle bounds policy. You can also create additional monitoring policies.

In the policy, you can specify lower and upper thresholds, as well as event tracking method: by frequency (EPS) or by quantity. When the indicators reach the values specified in the applied monitoring policy, a monitoring event with the information about the event source is generated, and an email notification is sent. One or more monitoring policies can be applied to an event source.

Monitoring policies are displayed in the KUMA web interface under **Source status** on the **Monitoring policies** tab.

Tools for monitoring event sources:

The status of sources can be monitored in several ways:

- List of event sources

  In KUMA you can monitor the status of sources, data from which are sent to the collectors. Collectors are used to generate lists of sources, which then are merged in the KUMA Core and displayed in the **Source status** section, on the **List of event sources** tab of the solution web interface. Information about event sources is updated every minute.

  You can track the state of each source by its status. The source status is determined by the settings of the monitoring policy assigned to that source.

- Email notifications

  When the monitoring policy is triggered, a corresponding notification is sent to an email address. You can configure notifications when creating or modifying a monitoring policy.

- Widgets and reports

  If the event stream from a source exceeds the thresholds specified in the monitoring policy, KUMA creates a stream monitoring informational event of type 5 (`Type=5`). You can specify this event type in a query to search for such events in the database:

  ```
  SELECT * FROM 'events' WHERE Type=5
  ```

  Based on this search criterion, you can create widgets of the **Cvents** type to visualize the status of sources on the dashboard. The created widgets can be added to a report template, and you can configure scheduled delivery of the report via email.

- Alerts.

  You can create a correlation rule that triggers when a monitoring event (`Type=5`) is generated, and link this rule to the correlator. In this case, when a monitoring event is created, an alert is generated.

Example of configuring event source monitoring

Configuring of event source monitoring in an infrastructure with domain controllers, Kaspersky Security Center servers, and workstations consists of the following steps:

1. **Creating monitoring policies**

   Create monitoring policies for domain controllers, Kaspersky Security Center servers, and workstations.

   For domain controllers, set the minimum event stream to 100 events per second.

   For Kaspersky Security Center servers, set the minimum event stream to 100 events per hour.

   For workstations, set the minimum event stream to 1 event per hour. Also, enable the **Set up a schedule by days of the week** toggle switch and specify only weekdays.

2. **Configuring notifications**

   For each policy, specify an email address for sending notifications, as well as a notification template.

3. **Enabling monitoring policies for event sources**

   Assign a corresponding monitoring policy to each event source.

A list of event sources is generated. For each of the sources, the event stream is monitored individually. For example, if KUMA stops receiving data from a domain controller, the administrator receives an email notification, and a stream monitoring informational event of Type 5 (`Type=5`) is sent to the KUMA storage. To track such events, you can create widgets, reports, and alerts.

Determining event sources

You can configure automatic identification of event sources using one of the following sets of fields:

- **Custom set of fields**. You can specify up to nine fields in the required order. You don't have to specify the `TenantID` field, because it is determined automatically.

- **Default set of fields**: `DeviceProduct`, `DeviceHostName`, `DeviceAddress`, `DeviceProcessName`. The order of the fields cannot be changed.

  Sources are determined if the `DeviceProduct` + `DeviceAddress` or `DeviceHostname` + `TenantID` fields (the value is defined automatically) in the events contain non-empty values. The `DeviceProcessName` field can be empty. If the `DeviceProcessName` field is not empty, and the other required fields are filled, the solution identifies a new source.

Event sources identification algorithm based on values in event fields

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (determined automatically)	
✓	✓			✓	Source 1 identified
✓		✓		✓	Source 2 identified
✓	✓	✓		✓	Source 3 identified
✓	✓		✓	✓	Source 4 identified
✓		✓	✓	✓	Source 5 identified
✓	✓	✓	✓	✓	Source 6 identified

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (determined automatically)	
	✓	✓		✓	Source not identified
	✓		✓	✓	Source not identified
		✓	✓	✓	Source not identified
✓			✓	✓	Source not identified

How to configure event source determination

Only one field set is used to monitor an event source within a single KUMA instance. When KUMA is updated to a new version, the default set of fields is applied.

Only users with the General administrator role can configure a set of fields for identifying an event source.

To configure the determination of event sources:

1. In the KUMA web interface, go to the **Source status** section.
2. On the **List of event sources** tab in the menu ⋮, click **Settings**.
3. In the **Settings of event source detection** window that opens, do one of the following:
   - If you want to configure a custom set of fields, in the Grouping fields**Grouping fields for determining the source**, select the event fields by which you want to identify event sources.

     You can specify up to nine fields in the required order. KUMA will identify sources in which the `TenantID` field is filled (determined automatically) and at least one field from the **Grouping fields for determining the source** list. For numeric fields, 0 is considered an empty value. If a single numeric field is selected for source identification, and the value of the numeric field is 0, the source is not detected.
   - If you want to select a default set of fields, click **Apply default mapping**.

     The default order of fields cannot be changed. If you manually specify the fields in the wrong order, an error will be displayed and the button to save settings will become unavailable. The correct default sequence of fields is: `DeviceProduct`, `DeviceHostName`, `DeviceAddress`, `DeviceProcessName`. A minimum configuration for identifying event sources using the default set of events is: non-empty values in the `DeviceProduct` + `DeviceAddress` and/or `DeviceHostName` + `TenantID` fields (TenantID is determined automatically).
4. Click **Save**.

   Once you have saved the modified set of fields, an audit event is created and all previously identified sources are deleted from the KUMA web interface and from the database; the assigned monitoring policies are disabled.
5. Restart the collectors to apply the changes and begin identifying event sources by the specified list of fields.

Source identification is configured.

To view events that are associated with an event source:

1. In the KUMA web console, go to **Source status** → **List of event sources**, then click the arrow icon > in the row of the required event source.

   The event arrival schedule opens under the source line.

2. Click the link **Events in <number> days**.

The **Events** section opens, displaying a list of events for the selected source for the last five minutes. Values of fields configured in the event source identification settings are automatically specified in the query. If necessary, in the **Events** section, you can change the time period in the query and click **Run query** again to view queried data for the specified time period.

Limitations

When identifying sources, the following restrictions apply:

- If default set of fields is used, KUMA registers the event source provided that the raw event contains the `DeviceProduct` + `DeviceAddress` and/or `DeviceHostName` fields.

  If the raw event does not contain the `DeviceProduct` + `DeviceAddress` and/or `DeviceHostName` fields, you may perform the following actions:

  - Configure enrichment in the normalizer. To do this, in the **Enrichment** tab of the normalizer, select the **Event** data type, specify the **Source field** setting, and for the **Target field** setting select the `DeviceProduct` + `DeviceAddress` and/or `DeviceHostName` and click **OK**.

  - Use an enrichment rule. To do this, select the **Event** data source type, specify the **Source field** setting, and for the **Target field** setting select `DeviceProduct` + `DeviceAddress` and/or `DeviceHostName`, then click **Create**. The created enrichment rule must be linked to the collector at the "Event enrichment" step.

  KUMA will perform enrichment and register the event source.

- If KUMA receives events with identical values of the fields that identify the source, KUMA registers different sources if the following conditions are satisfied:

  - The values of the required fields are identical, but different tenants are determined for the events.

  - The values of the required fields are identical, but one of the events has an optional `DeviceProcessName` field specified.

  - The values of the required fields are identical, but the data in these fields have different character case.

  If you want KUMA to log such events under the same source, you need to configure the fields in the normalizer.

Viewing information about event sources

To view event sources,

in the KUMA web interface, go to the **Source status** section.

The event sources table is displayed.

You can use the **Search** field to search for event sources. To search using a single character, enter that character and press **Enter**.

You can sort the table by clicking the column heading of the relevant parameter and selecting **Ascending** or **Descending**. You can also filter the table by the **Status** or **Monitoring policy** columns by clicking the relevant column's heading and selecting the values that need to be displayed.

To track changes in the list of sources, you can configure the data update interval in the table. Available update periods: **1 minute**, **5 minutes**, **15 minutes**, **30 minutes**, **1 hour**. The default value is **No refresh**.

The event sources table contains the following columns:

- **Status**—status of the event source:
  - Green—events are received within the limits of the assigned monitoring policies.
  - Red—the frequency or number of incoming events go beyond the limits defined in at least one assigned monitoring policy.

    In this case, a Monitoring event is generated. The monitoring event is generated in the tenant that owns the event source and is sent to the Main tenant's storage (this storage must already be deployed in the Main tenant). If you have access to the tenant of the event source and do not have access to the Main tenant, you can still search for monitoring events in the Main tenant's storage; the monitoring events of the tenants available to you will be displayed. You can also configure notifications to be sent to the specified email address.
  - Gray—monitoring policies have not been assigned to the event source.
- **Name**—name of the event source. The name is generated automatically from the values of fields configured in the event source identification settings.

  You can rename an event source by hovering over its name and clicking the pencil icon. The name can contain no more than 128 Unicode characters.
- **Host name or IP address**—a name or IP address of the host from which the events originate, if the `DeviceHostName` or `DeviceAddress` fields are specified in the event source identification settings.
- **Monitoring policy**—list of the monitoring policies assigned to the event source.

  If you want to filter the list of event sources by applied monitoring policies, click the name of this column and select one or more monitoring policies. If necessary, you can find policies in the list using the **Search** field. To find a policy by searching for a single character, enter that character and press **Enter**.

  You can view information about all monitoring policies assigned to an event source by clicking the row of the source. This opens a window that displays the settings of monitoring policies, as well as the status of the source according to each policy. If several monitoring policies are assigned to the source and a red status is displayed for it, in this window you can determine which policy was triggered. You can also see which policies are enabled and which are disabled, and when the disabled policies will be enabled again.
- **Stream**—frequency at which events are received from the event source.

  If a source is assigned monitoring policies of the **quantity of received events** type only or monitoring policies of different types, then sources with an event count are displayed in the **Flow** field. If a source is assigned monitoring policies of the **event reception frequency** type only or no monitoring policies, sources with an event count per second are displayed in the **Flow** field.

  Sorting by the **Stream** column first displays the sources with the **event reception frequency** policy type, and then the sources with the **number of events per second**.

After receiving the user's request, KUMA selects event sources and sorts them using the values from the **Flow** column at the time of receiving the request. After that, the values in this column are updated in accordance with the user's request.

> The displayed value may not match the sorting order because event data in event sources is dynamically updated to provide up-to-date information.

- **Tenant**—the tenant that owns the events received from the event source.

Viewing the dynamics of incoming events

You can examine the dynamics of events received from an event source over the last seven days with respect to the applied monitoring policies in one of the following ways:

- View the graph for an individual event source.
- Plot a chart based on graphs for multiple sources.

  A chart based on graphs for several event sources may be required, for example, to compare the activity of event sources of the same type that are expected to behave similarly but, in practice, show different behavior.

Viewing the graph for an individual event source

To view the graph for an individual event source,

In the KUMA web console, go to **Source status** → **List of event sources**, then click the arrow icon > in the row of the required event source.

The event arrival schedule opens under the source line.

The data in the graph is displayed as follows:

- The data is displayed for the days on which the events were received. The maximum period is seven days.

  In the upper left corner above the graph the number of days will be displayed, and in the upper right corner the data display period is shown. You can view the list of events for the selected source by clicking the **Events for <number> days** button. The **Events** section opens, displaying a list of events for the selected source for the last five minutes.

  In monitoring events, the name of the triggered monitoring policy is written to the `message` field. If you specified the `message` field as one of the fields that are used to identify event sources, then when a monitoring policy is triggered, KUMA overwrites the value of this field and indicates the name of the monitoring policy in it. In this case, when you go to the **Events** section, the monitoring events for the selected source are not included in the selection of events and are not displayed.

- The X-axis represents days, and the Y-axis represents the frequency of events (EPS).

- The lines represent the average, maximum, and minimum number of events for every 15-minute period during the last 7 days.

  If you want to view the number of events at a specific time, hover over a point on the graph. The data on the average, maximum, and minimum number of events at a specific date and time are displayed.

Creating a diagram for several event sources

To plot a chart based on graphs for multiple event sources:

1. In the KUMA web console, under **Source status** → **List of event sources**, select the check boxes next to one or more event sources.

   > You can plot a chart for up to 5 event sources at the same time.

2. In the toolbar or menu (⋮), click the **Build chart** button.

   The displayed **Chart** pane contains a chart of incoming events for all selected sources, as well as a table that displays the current number of events, the maximum number of events, and the average number of events for each source, calculated based on the data from the chart. You can compare how the data for the selected sources relates to each other over time.

   The data in the chart is displayed as follows:

   - The data is displayed for the days on which the events were received. The maximum period is seven days.

     In the upper right corner above the chart, the period for which data is displayed is indicated.

   - The X-axis represents days, and the Y-axis represents the frequency of events (EPS).

   - The lines in the chart represent the average number of incoming events from the selected event sources for every 15-minute interval during the last 7 days.

     You can hover over the chart to view the average number of events for each source at a specific time.

3. If you want to hide event sources in the chart, clear the check boxes next to the corresponding event sources in the table below the chart.

4. If you want to zoom in on the chart and open it in full screen, click the double-arrow icon ↙↗.

Exporting event source information to a CSV file

You can export information about one or more event sources and the monitoring policies applied to them as a CSV file (comma-separated) in UTF-8 encoding. For each monitoring policy applied to a source, the file contains the following parameters: **Status**, **Name**, **Monitoring policy**, **Lower limit**, **Upper limit**, **Stream**, **Tenant**. If multiple monitoring policies are applied to a source, each monitoring policy and its parameters starts on a new line. Grouping fields for source identification are saved in the CSV file in the order specified at the source identification setup stage. When exporting data for multiple sources, the order of sources configured in the KUMA web interface is not preserved. If you want to sort the list of sources, you can do so in Excel or use grep with sorting.

To export event source data to a CSV file:

1. In the KUMA web console, under **Source status** → **List of event sources**, select the check boxes next to one or more event sources.

   In the lower left part of the table, you can find the number of selected sources and the total number of sources in the table. You can select up to 150,000 event sources.

   You can also select the check box in the header of the first column of the table and select one of the following options:

   - **Select all**—to select all event sources on all pages of the table. If you have used search to filter sources, this will select all sources that match the search query. However, you cannot clear the check box for an individual event source.

   - **Select all in page**—to select all event sources on the currently displayed page. If you have used search to filter sources, this will select all sources on the currently displayed page that match the search query. After selecting all sources on the page, you can clear the check boxes for individual event sources.

2. In the toolbar or menu (⋮), click **CSV**.

   An event source export task is created in the task manager.

3. Go to the **Task manager** section and find the created task.

   When the file is ready, the **Status** column of the task displays the **Completed** status.

4. Click the task type name and select **Download** from the drop-down list.

The CSV file with event source information is downloaded in accordance with your browser settings. The default file name is `event-source-list_YYYYMMDD_HHMMSS.csv`.

Removing an event source

Event sources can be deleted from the table. Statistics on deleted sources are also deleted. If a collector continues to receive data from the source, the event source will re-appear in the table but its old statistics will not be taken into account.

To delete an event source from the table:

1. In the KUMA web console, in the **Source status** → **List of event sources** section, select one or more event sources in the table by selecting the corresponding check boxes in the first column.

   In the lower left part of the table, you can find the number of selected sources and the total number of sources in the table. You can select up to 150,000 event sources.

   You can also select the check box in the header of the first column of the table and select one of the following options:

   - **Select all**—to select all event sources on all pages of the table. If you have used search to filter sources, this will select all sources that match the search query. However, you cannot clear the check box for an individual event source.

     If you need to delete all event sources, but the table has not been updated for some time, the sources added during this period may not be displayed in the table, but they still will be deleted.

   - **Select all in page**—to select all event sources on the currently displayed page. If you have used search to filter sources, this will select all sources on the currently displayed page that match the search query. After selecting all sources on the page, you can clear the check boxes for individual event sources.

2. In the toolbar or menu (⋮), click the **Delete** button.

   If you delete more than 100,000 event sources to which a filter or search was applied, only the first 100,000 event sources will be deleted. You can select all filtered event sources again and delete them, and then repeat this until you have deleted all event sources that you intended to delete. You can delete over 100,000 event sources if no filters or searches are applied to them by selecting sources using the **Select all** button.

Algorithm for monitoring policy application

Monitoring policies are applied to an event source in accordance with the following algorithm:

1. The event stream is counted at the collector.

2. The KUMA Core server obtains information about the stream from collectors every 15 seconds.

3. The collected data is stored on the KUMA Core server in a VictoriaMetrics time-series database. Data retention period on the KUMA Core server is 15 days.

4. An inventory of event sources is taken once per minute.

5. The stream is counted separately for each event source in accordance with the following rules:

   - If a monitoring policy is applied to the event source, the displayed maximum number of event stream is calculated in accordance with the currently applied monitoring policies for the time interval specified in the policy.

     Depending on the policy type, the number of the event stream is counted based on number of events (for the **quantity of received events** policy type or policies of different types) or number of events per second (EPS, for the **event reception frequency** policy type). You can look up how the stream is counted for the applied policy in the **Stream** column on the **List of event sources** page.

   - If no monitoring policy is applied to the event source, the number for the event stream corresponds to the last value.

6. Once a minute, the application checks if any monitoring policies exist that must be applied to event sources or stopped according to the monitoring policy schedule.

7. Once a minute, the stream of events is checked for compliance with policy settings.

If the event stream from the source crosses the thresholds specified in the monitoring policy, information about this is recorded in the following way:

- A notification about a monitoring policy getting triggered is sent to the email addresses specified in the policy. You can also configure a notification template for each policy.

- A stream monitoring informational event of type `5` (`Type=5`) is generated. The event contains fields described in the table below.

Fields of the monitoring event

Event field name	Field value
`ID`	Unique ID of the event.
`Timestamp`	Event time.
`Type`	Type of the audit event. For the audit event, the value is `5` (monitoring).
`Name`	Name of the monitoring policy.

Event field name	Field value
`DeviceProduct`	`KUMA`
`DeviceCustomString1`	The value from the `value` field in the notification. Displays the value of the metric for which the notification was sent.

The generated monitoring event is sent to the following resources:

- All storages of the Main tenant
- All correlators of the Main tenant
- All correlators of the tenant in which the event source is located

Viewing monitoring policies

To view the monitoring policies for event sources:

In the KUMA web interface, go to the **Source status** → **Monitoring policies** section.

The Monitoring policy table is displayed.

You can use the **Search** field to look for monitoring policies. The search is performed in the following columns: **Name**, **Tenant**, **Type**, **Schedule** (day and time). To find a policy by searching for a single character, enter that character and press **`Enter`**.

You can sort the table by clicking the column header of the relevant setting. The maximum size of the policy list is not limited.

The event sources table contains the following columns:

- **Name** is the name of the monitoring policy.
- **Lower threshold** is the minimum allowed number of events received from the source.
- **Upper threshold** is the maximum allowed number of events received from the source.
- **Interval** is the frequency at which the VMalert service queries VictoriaMetrics for policy data while it is being applied to the event source.
- **Type** is the way to track events: by frequency (EPS) or by number.
- **Tenant** is the tenant that owns the monitoring policy.
- **Sources** allows to open the table of event sources by clicking the **Show** link; sources in the table are filtered by the selected policy.
- **Schedule** shows how often the monitoring policy is applied to event sources.
- **Policy update status** shows whether the monitoring policy is **Updated** or **Update required**.
- **Last applied policy** shows date and time when the policy was last applied to event sources.

Creating a monitoring policy

To add a new monitoring policy:

1. In the KUMA web interface, in the **Source status** → **Monitoring policies** section, click **Add**.

2. In the **Policy name** field, enter the name of a policy you are creating. The name must contain from 1 to 128 Unicode characters and must be unique within the selected tenant.

   We recommend naming the policy to reflect the schedule that you configured in the monitoring policy settings.

3. In the **Tenant** drop-down list, select the tenant that you want to own the policy.

   Your tenant selection determines event sources that can be covered by the monitoring policy.

4. For the **Type** settings, select how events will be counted:

   - **by count**—by the number of events over a certain period of time.

   - **by EPS**—by the number of events per second (EPS) over a certain period of time. The average value over the entire period is used. You can also track spikes at specific periods of time.

5. In the **Count interval** field, specify the period during which the monitoring policy must take into account the data from the monitoring source. You can use the drop-down list on the right to select a value in minutes, hours, or days. The maximum value is 14 days.

6. If you selected the **by EPS** policy type, in the **Control interval, minutes** field, specify the period of time (in minutes) within which checks must record a deviation in the number of event flows from the norm for the monitoring policy to be triggered:

   - If, during this time period, all checks (performed once per minute) find that the stream is crossing the threshold, the monitoring policy is triggered.

   - If, during this time period, one of the checks (performed once per minute) finds that the stream is within the thresholds, the monitoring policy is not triggered, and the count of check results is reset.

   If you do not specify the frequency of measurement, the monitoring policy is triggered immediately after the stream is found to cross the threshold.

7. In the **Lower limit** and **Upper limit** fields, define the thresholds representing normal behavior. Deviations then will trigger the monitoring policy to create an alert and send notifications.

   The **Lower threshold** field must be filled.

8. In the **Evaluation interval** field, specify the frequency with which the VMalert service will query VictoriaMetrics for policy data while the policy is being applied to the event source. You can use the drop-down list on the right to select a value in minutes, hours, or days. The default evaluation interval is 5 minutes.

   When specifying the evaluation interval, keep in mind the policy schedule. For example, if you configured the policy to be applied once every few hours, we do not recommend configuring a short interval and causing excessive load on VictoriaMetrics.

9. If necessary, in the **Send notifications** field, specify email addresses to which notifications about the KUMA monitoring policy triggers must be sent. To add an address, enter it in the field and press **`Enter`** or click **Add**. You can specify multiple email addresses.

   To forward notifications, you need to configure an SMTP server connection.

10. In the **Notification template** drop-down list, select the template that you want to use for notifications. If necessary, click the **Create** button to start creating a new notification template.

    By default, the basic notification template is selected. You can reset the template selection and switch to the base template by clicking the X icon.

11. In the **Schedule** section, configure how often you want to apply the monitoring policy to event sources. By default, the policy is applied every week, every day, from 00:00 to 23:59. To configure the monitoring policy schedule, do some of the following:

    - If you want to apply the monitoring policy weekly on specific days of the week:

      a. Enable the **Set up a schedule by days of the week** toggle switch.

      b. In the **Days of week** drop-down list, select the days of the week on which you want the policy to be applied to the source.

      If you want to clear the selection, click the X icon.

      c. In the **Time** field, specify the start and end time of the policy, with minute precision.

      The bounds of the specified range are included. For example, if the end time is set to 23:59, the policy will be applied until 23:59:59.999. The default interval is 00:00 to 23:59. The start time must be earlier than the end time.

      d. If you want to add another period, click the **Add period** button and repeat steps 'b' and 'c'.

      You can add any number of periods.

    - If you want to apply the monitoring policy on specific dates:

      a. Enable the **Set up a schedule for specific days** toggle switch.

      b. Click **Days of the month**, and use the calendar to select the dates for the policy to be applied to the source. You can select a period of several days or an individual day. The start date of the period must be earlier than the end date of the period.

      The dates are configured without a year value, so the policy will be applied annually on the specified days until you delete this period. If you want to clear the selection, click the X icon.

      c. In the **Time** field, specify the start and end time of the policy, with minute precision.

      The bounds of the specified range are included. For example, if the end time is set to 23:59, the policy will be applied until 23:59:59.999. The default interval is 00:00 to 23:59. The start time must be earlier than the end time.

      d. If you want to add another period, click the **Add period** button and repeat steps 'b' and 'c'.

      You can add any number of periods.

If you applied a schedule by day of the week and by day of the month at the same time, the day-of-the-month policy is applied first.

12. Click **Add**.

The monitoring policy is created. The policy must now be applied to the event source.

Applying monitoring policies

To apply monitoring policies to event sources:

1. In the KUMA web console, in the **Source status** → **List of event sources** section, select the check boxes next to one or more event sources for which you want to enable monitoring policies.

   You can also select the check box in the header of the first column of the table and select one of the following options:

   - **Select all** to select all event sources on all pages of the table. If you have used search to filter sources, this will select all sources that match the search query. However, you cannot clear the check box for an individual event source.
   - **Select all in page** to select all event sources on the currently displayed page. If you have used search to filter sources, this will select all sources on the currently displayed page that match the search query. After selecting all sources on the page, you can clear the check boxes for individual event sources.

   In the lower left part of the table, you can find the number of selected sources and the total number of sources in the table.

2. Click the **Enable policy** button.

3. This opens the **Apply policy** window; in that window, select one or more monitoring policies that you want to apply to the selected event sources. The table lists only monitoring policies that you can assign to the selected sources. These are the policies that belong to the same tenant or to the Shared tenant (if you have access to it). If no shared policies exist for the selected event sources and you do not have access to the Shared tenant, the policy table will be empty.

   To select all available policies, select the check box in the first column's header. You can also use context search by policy name or sort the policies by clicking the heading of the column by which you want to sort the table and selecting **Ascending** or **Descending**.

   Search or sorting is not available for the **Sources**, **Schedule**, **Policy update status**, **Date the policy was last applied** columns.

4. Click **Apply**.

5. In the table of sources, click **Update policy** to apply the changes to event sources.

The monitoring policies are applied to the selected event sources; the status of these sources changes to green. The names of the policies applied to the sources are displayed in the **Monitoring policy** column. A message is also displayed indicating the number of sources to which the policies have been applied. If a monitoring policy is triggered for an event source, the status of the source is updated after you refresh the page manually or automatically. We recommend configuring an automatic data refresh period to keep track of changes in the list of sources.

If you have selected more than 100,000 event sources and applied one or more policies to them, these policies are applied only to the first 100,000 sources to which these policies have not yet been applied. If you need to apply policies to the remaining sources, you can do one of the following:

- Select all sources again and apply the policies to them.
- Filter the table of sources by any parameter so that the table displays less than 100,000 sources, then apply the policies to them.

Repeat the action until the policies have been applied to all the sources that you need.

Modifying and updating a monitoring policy

To change a monitoring policy:

1. In the KUMA web interface, go to the **Source status** → **Monitoring policy** and click the monitoring policy that you want to change.

   The **Policy settings** window opens.

2. Modify the settings as necessary, then click **Save**.

If a monitoring policy is applied to an event source, it must be updated whenever the following policy settings are changed:

- **Policy name**
- **Type**.
- **Lower limit**
- **Upper limit**
- **Count interval**
- **Control interval**
- **Evaluation interval**
- **Schedule**

Schedule changes are applied within a minute, when KUMA checks for policies that need to be enabled or disabled.

Every 30 minutes, KUMA checks if any monitoring policies require updating, and if that is the case, it automatically runs a task to update those monitoring policies. You can also run the update task manually by clicking the **Update policy** button at the top of the table. One task updates all policies that need updating.

> While the policy update task is running, the **Update policy** button is unavailable for all users. If another user has edited the settings of the policy that necessitate an update, the **Update policy** button becomes active for you only after you refresh the page or edit the policy or an event source.

Information about updating monitoring policies is displayed in the **Policy update status** column:

- **Update required**—one of the monitoring policy settings was edited, but the changes have not been applied to event sources.
- **Updated** in any of the following cases:
  - After editing the policy, the task to apply the policy was started, and the changes were applied to event sources.
  - You have edited one of the following policy settings, which does not require starting the update task:
    - **Send notifications**
    - **Notification template**

    In this case, the edited policy settings are applied to event sources after a minute. Changes of the **Notification template** setting are applied instantly.
  - The modified monitoring policy is not applied to event sources.

Disabling monitoring policies

To disable monitoring policies for event sources:

1. In the KUMA web console, in the **Source status** → **List of event sources** section, select the check boxes next to one or more event sources for which you want to disable monitoring policies.

   You can also select the check box in the header of the first column of the table and select one of the following options:

   - **Select all** to select all event sources on all pages of the table. If you have used search to filter sources, this will select all sources that match the search query. However, you cannot clear the check box for an individual event source.
   - **Select all in page** to select all event sources on the currently displayed page. If you have used search to filter sources, this will select all sources on the currently displayed page that match the search query. After selecting all sources on the page, you can clear the check boxes for individual event sources.

   In the lower left part of the table, you can find the number of selected sources and the total number of sources in the table.

2. Click **Disable policy**.

3. This opens the **Disable policy** window; in that window, select one or more monitoring policies that you want to disable for the selected event sources. The table lists all monitoring policies applied to at least one of the selected event sources.

   To select all available policies, select the check box in the first column's header. You can also use context search or sort the policies by clicking the heading of the column by which you want to sort the table and selecting **Ascending** or **Descending**.

   Search or sorting is not available for the **Sources**, **Schedule**, **Policy update status**, **Date the policy was last applied** columns.

4. In the settings section above the policy table, do one of the following:

   - If you want to temporarily suspend the policies, select **For** and specify the time in minutes, hours, or days after which the selected policies will be reapplied to event sources. Maximum values:

     - For days: 30

     - For hours: 743

     - For minutes: 44579

   - If you want to permanently disable the selected policies for event sources, select **Until you enable the policy manually**.

   The default selection is **For**, and the value is set to **5 minutes**.

5. Click **Disable**.

6. In the table of sources, click **Update policy** to apply the changes to event sources.

   The monitoring policies will be disabled for selected event sources or suspended for the specified time period. The status of these sources changes to gray. A message is displayed indicating the number of sources for which the policies have been disabled.

If you have selected more than 100,000 event sources and disabled one or more policies for them, these policies are disabled only for the first 100,000 sources to which these policies are applied. If you need to disable policies for the remaining sources, you can do one of the following:

- Select all sources again and disable the policies for them.

- Filter the table of sources by any parameter so that the table displays less than 100,000 sources, then disable the policies for them.

  Repeat the action until the policies have been disabled for all the sources that you need.

Creating a monitoring policy based on an existing one

To create a new monitoring policy based on an existing one:

1. In the web interface, open the **Source status** → **Monitoring policies** section.

2. Select the check box next to the monitoring policy based on which you want to create a new policy.

   If necessary, you can find monitoring policies in the list using the **Search** field. The search will be performed in the following columns: **Name**, **Tenant**, **Type**, **Schedule** (day and time). To find a policy by searching for a single character, enter that character and press **`Enter`**.

3. Click **Duplicate policy**.

4. In the **Add policy** window that opens, specify policy settings.

   By default, the `- copy` suffix is appended to the name of a new policy.

5. Then click the **Add** button.

The monitoring policy is created based on an existing policy.

Deleting monitoring policies

> You cannot remove predefined monitoring policies or policies that are assigned to data sources.

To delete a monitoring policy:

1. In the KUMA web interface, in the **Source status** → **Monitoring policies** section, select one or more monitoring policies that you want to delete.

   If necessary, you can find monitoring policies in the list using the **Search** field. The search will be performed in the following columns: **Name**, **Tenant**, **Type**, **Schedule** (day and time). To find a policy by searching for a single character, enter that character and press **`Enter`**.

2. Click **Delete policy** and confirm the action.

The selected monitoring policies are deleted.

Integration with other solutions

In this section, you'll learn how to integrate KUMA with other solutions to enrich its functionality.

Integration with Kaspersky Security Center

You can configure integration of KUMA with Kaspersky Security Center Windows and Kaspersky Security Center Linux. In the following instructions, Kaspersky Security Center stands for the application that you have chosen for integration.

You can configure integration with selected Kaspersky Security Center servers for one, several, or all KUMA tenants. If Kaspersky Security Center integration is enabled, you can import information about the assets protected by this application, manage assets using tasks, and import events from the Kaspersky Security Center event database.

> First, you need to make sure that the needed Kaspersky Security Center server allows an incoming connection for a KUMA hosting server.

To learn more about configuring integration with Kaspersky Security Center, watch the video below and then follow the step-by-step instructions.

https://www.youtube.com/watch?v=-MYOlw0sPiY

Configuring KUMA integration with Kaspersky Security Center includes the following steps:

1. **Creating a user account in the Kaspersky Security Center Administration Console**

   The credentials of this account are used when creating a secret to establish a connection with Kaspersky Security Center.

   The secret (account role in Kaspersky Security Center) for integrating KUMA with Kaspersky Security Center must be created with consideration of how the hierarchy of the Administration Server is organized (availability of virtual servers, server administration features, etc) and types of devices that the Administration Server will manage (OS, type: servers, mobile devices, etc). All these nuances are regulated and configured on the Kaspersky Security Center side.

   The following actions can be performed in KUMA on assets from Kaspersky Security Center:

   - Starting a task of the **Update** type.
   - Starting a task of the **Virus Scan** type.
   - Moving assets between Kaspersky Security Center groups.
   - Accepting software updates (to fix a vulnerability of an asset in Kaspersky Security Center).

   To be able to perform the actions listed above, you can use a predefined account in Kaspersky Security Center with the Main Administrator role. In this case, you do not need to add permissions manually.

   You can also use the Kaspersky Endpoint Security Administrator predefined role in Kaspersky Security Center, but in that case, you must additionally grant access to the following functionality:

   1. Management of administration groups
   2. Vulnerability and patch management

      Some additional permissions may be required depending on the configuration of Kaspersky Security Center.

   Minimum permissions for integration with Kaspersky Security Center:

   - "Access objects regardless of their ACLs" allows you to import Kaspersky Security Center assets into KUMA.

   - "Management of administration groups" allows you to move assets between groups in Kaspersky Security Center from the KUMA interface.

   - "Basic functionality" allows you to create and run tasks on Kaspersky Endpoint Security hosts.

For more details about creating a user account and assigning permissions to a user, please refer to the *Kaspersky Security Center Help Guide*.

2. **Adding the created user account to the list of exclusions for two-factor authentication**

   In the Kaspersky Security Center Administration Console, exclude the user account created for the integration of KUMA with Kaspersky Security Center from two-factor authentication in Kaspersky Security Center Windows or Kaspersky Security Center Linux.

3. **Creating a secret of the credentials type for connecting to Kaspersky Security Center**

4. **Configuring Kaspersky Security Center integration settings**

5. **Creating a connection to the Kaspersky Security Center server for importing information about assets**

   If you want to import information about assets registered on Kaspersky Security Center servers into KUMA, you need to create a separate connection to each Kaspersky Security Center server for each selected tenant.

   > If integration is disabled for the tenant or there is no connection to Kaspersky Security Center, an error is displayed in the KUMA web interface when attempting to import information about assets. In this case, the import process does not start.

Configuring Kaspersky Security Center integration settings

To configure the settings for integration with Kaspersky Security Center:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Select the tenant for which you want to configure integration with Kaspersky Security Center.

   The **Kaspersky Security Center integration** window opens.

3. Use the toggle switch in the **Status** column to enable or disable Kaspersky Security Center integration for the tenant.

   By default, Kaspersky Security Center integration for tenants is disabled.

4. Specify intervals for automatic import of asset information and asset vulnerability information from Kaspersky Security Center:

   a. Click the name of the tenant in the **Tenant** column.

   b. A sidebar is displayed; on this sidebar, in the **KSC assets, hardware information** field, enter the interval in hours for the automatic import of information about the basic attributes of assets (protection status, anti-virus database version, hardware). and must be an integer. The default setting is `1` (1 hour).

   c. In the **KSC assets attributes (vulnerabilities, software, owners)** field, enter the interval in hours for automatic import of information about other attributes of assets (vulnerabilities, software, owners). and must be an integer. The default setting is `12` (12 hours).

   Importing the information about asset attributes (vulnerabilities, software, owners) may involve downloading a large amount of data, which may take a longer time to complete, we recommend setting a longer interval than for the hardware information import.

If necessary, you can manually import asset information and asset vulnerability information from Kaspersky Security Center.

5. Click the **Save** button.

The Kaspersky Security Center integration settings for the selected tenant will be configured.

If the tenant you need is missing from the list of tenants, you need to add the tenant to the list of tenants.

Adding a tenant to the list for Kaspersky Security Center integration

To add a tenant to the list of tenants for integration with Kaspersky Security Center:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Click the **Add settings for a new tenant** button.

3. The **Kaspersky Security Center** sidebar is displayed; on this sidebar, in the **Tenant** drop-down list, select the tenant that you want to add.

4. Then click the **Add** button.

The selected tenant will be added to the list of tenants for integration with Kaspersky Security Center.

Removing a tenant from the list of tenants for Kaspersky Security Center integration

To remove a tenant from the list of tenants for Kaspersky Security Center integration:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Select the check box for the tenant that you want to delete.

3. Click the **Delete** button and confirm deletion.

The selected tenant is removed from the list of tenants for integration with Kaspersky Security Center.

Creating Kaspersky Security Center connection

To create a new Kaspersky Security Center connection:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Click the name of the tenant for which you want to create a Kaspersky Security Center connection.

3. A sidebar is displayed; on this sidebar, under **Connections**, click the **New** button and specify the following settings:

   - **Status** is the status of the connection to the selected Kaspersky Security Center server. You can use the toggle switch to enable or disable the connection. By default, the connection to the selected server is inactive. If this is the case, you cannot use this connection to connect to the Kaspersky Security Center server.

   - **Name** (required)—the name of the connection. The name can contain 1 to 128 Unicode characters.

   - **URL** (required) is the URL of the Kaspersky Security Center server. The default port is 13299.

   - In the **Secret** drop-down list, select the secret with the Kaspersky Security Center account credentials or create a secret.

     How to create a secret

     1. Click the plus (+) icon.

        The secret window is displayed.

     2. Enter information about the secret:

        a. In the **Name** field, choose a name for the added secret.

        b. In the **Tenant** drop-down list, select the tenant that will own the Kaspersky Security Center account credentials.

        c. In the **Type** drop-down list, select **credentials**.

        d. In the **User** and **Password** fields, enter the account credentials for your Kaspersky Security Center server.

        e. If you want, enter a **Description** of the secret.

     3. Click **Save**.

     You can change the selected secret by clicking the icon.

4. If necessary, select the **Vulnerability Management Integration** check box.

   Kaspersky Vulnerability Management integration settings

   a. In the **Vulnerability Management server URL** field, enter the address for connecting to the Kaspersky Vulnerability Management server. The address must be specified in the following format: `<ipv4_address or host_name>:<port>.` HTTPS is used by default; you do not need to specify it explicitly. The default port is 5054.

   b. In the **Maximum number of failed connection attempts** field, enter the number of unsuccessful attempts to get data from Kaspersky Vulnerability Management.

      If, after the specified number of attempts, KUMA is still unable to get data from Kaspersky Vulnerability Management, the solution automatically mode-switches to getting vulnerability data from Kaspersky Security Center. As soon as the connection is restored, KUMA switches back to getting data from Kaspersky Vulnerability Management. At each iteration of data retrieval, the new data overwrites the current data; the data is not merged.

      Possible values: 0 to 100. A value of 0 means that KUMA switches to getting vulnerability data from Kaspersky Security Center after the first unsuccessful attempt to connect to Kaspersky Vulnerability Management.

5. If you want KUMA to import only assets that are connected to secondary servers or included in groups:

   a. Make sure that the connection to the Kaspersky Security Center server is enabled.

   b. In the **Hierarchy** section, click the **Upload** button.

   c. Select the servers and groups from which you want to import asset information.

   d. If you want to import assets only from new groups, select the **Import assets from new groups** check box.

6. If you want KUMA to import information about the assets of all Kaspersky Security Center servers:

   a. Make sure that the connection to the Kaspersky Security Center server is enabled.

   b. If you want to import information about the basic parameters of assets, click the **Import KSC assets** button.

   c. If you want to import information about other parameters of assets, click the **Import KSC assets attributes** button.

7. Click **Save**.

The connection to the Kaspersky Security Center server is now created. It can be used to import information about assets from Kaspersky Security Center to KUMA and to create asset-related tasks in Kaspersky Security Center from KUMA.

Editing Kaspersky Security Center connection

To edit a Kaspersky Security Center connection:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Select the name of the tenant for which you want to configure Kaspersky Security Center integration.

   This opens the **Kaspersky Security Center** window.

3. Click the name of the Kaspersky Security Center connection you want to edit.

   The window with the selected Kaspersky Security Center connection parameters opens.

4. Make the necessary changes to the settings.

5. Click the **Save** button.

The Kaspersky Security Center connection will be changed.

Deleting Kaspersky Security Center connection

To delete a Kaspersky Security Center connection:

1. Open the KUMA web interface and select the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Select the name of the tenant for which you want to configure Kaspersky Security Center integration.

   This opens the **Kaspersky Security Center** window.

3. Select the Kaspersky Security Center connection that you want to delete.

4. Click the **Delete** button.

The Kaspersky Security Center connection will be deleted.

Importing events from the Kaspersky Security Center database

In KUMA, you can receive events from the Kaspersky Security Center SQL database. Events are received using the collector, which uses the following resources:

- Predefined [OOTB] KSC MSSQL, [OOTB] KSC MySQL, or [OOTB] KSC PostgreSQL connector.
- Predefined [OOTB] KSC from SQL normalizer.

To learn more about event importing from the Kaspersky Security Center database, watch the video below, and then follow the step-by-step instructions.

https://www.youtube.com/watch?v=ikOEyl3fa18

To configure the import of events from Kaspersky Security Center:

1. Create a copy of the predefined connector corresponding to the type of database used by Kaspersky Security Center:

   a. In the KUMA web interface, in the **Resources** section, under **Resources**, select **Connectors**.

   b. Find the relevant predefined connector in the folder structure, select the check box next to this connector and click **Duplicate**.

   c. This opens the **Create connector** window; in that window, on the **Basic settings** tab, in the **Default query** field, if necessary, replace the KAV database name with the name of the Kaspersky Security Center database you are using.

   An example of a query to the Kaspersky Security Center SQL database

   SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

   ev.product_name AS product_name, ev.product_version AS product_version,

```
        ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As
msg,

CASE

       WHEN ev.rise_time is not NULL THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time )

          ELSE ev.rise_time

      END

   AS endTime,

   CASE

      WHEN ev.registration_time is not NULL

          THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )

          ELSE ev.registration_time

      END

   AS kscRegistrationTime,

   cast(ev.par7 as varchar(4000)) as sourceUserName,

   hs.wstrWinName as dHost,

   hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,

      CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

   CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

   CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +

   CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,

   serv.wstrWinDomain as kscNtDomain,

      CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

   CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

   CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +

   CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,

   CASE

   WHEN virus.tmVirusFoundTime is not NULL

          THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )
```

```
        ELSE ev.registration_time
      END
    AS virusTime,
    virus.wstrObject As filePath,
    virus.wstrVirusName as virusName,
    virus.result_ev as result
  FROM KAV.dbo.ev_event as ev
  LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId
  INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1
  Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus
  where registration_time >= DATEADD(minute, -191, GetDate())
```

d. In the **Connection** section, in the **Database kind** drop-down list, select the type of database you are using.

e. If necessary, select the **Secret separately** check box and enter the secret in the **Secret** field.

f. Place the cursor in the **URL** field and in the list that expands click the pencil icon (✎) in the row of the secret being used.

g. This opens the **Secret** window; in that window, in the **URL** field, specify the server connection address in the following format:

   `sqlserver://user:password@kscdb.example.com:1433/database`

   where:

   - `user`—user account with public and db_datareader rights to the required database.
   - `password`—user account password.
   - `kscdb.example.com:1433`—address and port of the database server.
   - `database`—name of the Kaspersky Security Center database. 'KAV' by default.

   Click **Save**.

h. In the **Create connector** window, in the **Connection** section, in the **Query** field, replace the 'KAV' database name with the name of the Kaspersky Security Center database you are using.

   This action is required if you want to use the **ID column** the query refers to.

   Click **Create**.

2. Install the collector to the KUMA web interface:

   a. Start the Collector Installation Wizard in one of the following ways:

      - In the KUMA web interface, in the **Resources** section, under **Services configuration**, click **Add event source**.

      - In the KUMA web interface, in the **Resources** section, under **Services configuration**, select **Collectors** and click **Add**.

   b. In the **Connect event sources** section, specify the name of the collector and select the tenant.

   c. In the **Transport** section, select the previously created connector.

   d. In the **Event parsing** section, click the **Add event parsing** button.

   e. This opens the **Basic event parsing** window; in that window, on the **Normalization scheme** tab, in the **Normalizer** drop-down list, select **[OOTB] KSC from SQL** and click **OK**.

   f. Specify other collector settings, if necessary. To import events, configuring settings in the other sections of the **Create collector** window is not required.

   g. In the **Setup validation** section, click **Create and save service**.

   h. Copy the command that appears in the lower part of the window. The command is required to install the collector on the server.

   i. Click **Save collector**.

3. Install the collector on the server.

   To do so, on the server on which you want to receive Kaspersky Security Center events, run the command that you copied to the clipboard after creating the collector in the web interface.

   As a result, the collector is installed and can receive events from the SQL database of Kaspersky Security Center.

You can view Kaspersky Security Center events in the **Events** section of the KUMA web interface.

Kaspersky Vulnerability Management integration

Kaspersky Vulnerability Management is a solution for managing vulnerabilities in an organization's IT infrastructure. This solution allows searching, analyzing, and prioritizing vulnerabilities detected on your assets.

When integration is configured, Kaspersky Vulnerability Management sends the following data to KUMA:

- Information about vulnerabilities detected on assets.

- List of applications installed on assets.

The resulting data allows timely identification and response to threats.

In KUMA, you can receive data about vulnerabilities and installed applications from Kaspersky Security Center and from Kaspersky Vulnerability Management. However, data must come from only one of these solutions. When integration with Kaspersky Vulnerability Management is enabled, data is received only from that solution. When the Kaspersky Vulnerability Management integration is disabled, data is received from Kaspersky Security Center.

KUMA adds the data received from Kaspersky Vulnerability Management to asset properties in the **Software info** and **Kaspersky Security Center vulnerabilities** sections.

Before you begin

For integration with Kaspersky Vulnerability Management, you need to configure and enable integration with Kaspersky Security Center and configure the connection to Kaspersky Security Center. When integration with Kaspersky Security Center is disabled, integration with Kaspersky Vulnerability Management also becomes disabled.

You must have a Tier 1 Analyst, Tier 2 Analyst, Tenant Administrator, or General Administrator role. If you have been assigned a custom role, KSC integration management must be made available to you in functional areas of your role.

Configuring the integration

To configure the Kaspersky Vulnerability Management integration:

1. In the web interface, open the **Settings** → **Integrations** → **Kaspersky Security Center** section.

   The **Kaspersky Security Center integration by tenant** window opens.

2. Select the tenant for which you want to configure Kaspersky Vulnerability Management integration, or click the **Add settings for a new tenant** button if you want to configure integration with Kaspersky Security Center for the new tenant.

   This opens the **Kaspersky Security Center** window.

3. Make sure the **Status** toggle switch is enabled.

4. In the **Connections** section, open an existing connection or create a new connection.

   If you use multiple connections, for example, if your organization has a hierarchy of Kaspersky Security Center Administration Servers, you need to configure Kaspersky Vulnerability Management integration for each of such connections.

5. Enable the **Vulnerability Management Integration** toggle switch.

6. In the **Vulnerability Management server URL** field, enter the address for connecting to the Kaspersky Vulnerability Management server. The address must be specified in the following format: `<ipv4_address or host_name>:<port>.` HTTPS is used by default; you do not need to specify it explicitly. The default port is 5054.

7. In the **Maximum number of failed connection attempts** field, enter the number of unsuccessful attempts to get data from Kaspersky Vulnerability Management.

If, after the specified number of attempts, KUMA is still unable to get data from Kaspersky Vulnerability Management, the solution automatically mode-switches to getting vulnerability data from Kaspersky Security Center. As soon as the connection is restored, KUMA switches back to getting data from Kaspersky Vulnerability Management. At each iteration of data retrieval, the new data overwrites the current data; the data is not merged.

Possible values: 0 to 100. A value of 0 means that KUMA switches to getting vulnerability data from Kaspersky Security Center after the first unsuccessful attempt to connect to Kaspersky Vulnerability Management.

8. Click **Save**.

Kaspersky Vulnerability Management integration is configured.

Kaspersky Endpoint Detection and Response integration

Starting with KATA 8.0, integration with Kaspersky Endpoint Detection and Response and the import of Kaspersky Endpoint Detection and Response telemetry into KUMA are no longer supported. Response through KEDR is not available, attempting to initiate response for an asset causes an error. Only the import of platform action events and alert events is available.

Kaspersky Endpoint Detection and Response (hereinafter also referred to as "KEDR") is a functional unit of Kaspersky Anti Targeted Attack Platform that protects assets in an enterprise LAN.

You can configure KUMA integration with Kaspersky Endpoint Detection and Response 4.0 or later to manage threat response actions on assets connected to Kaspersky Endpoint Detection and Response servers, and on Kaspersky Security Center assets. Commands to perform operations are received by the Kaspersky Endpoint Detection and Response server, which then relays those commands to the Kaspersky Endpoint Agent installed on assets.

To manage Kaspersky Endpoint Detection and Response actions on Kaspersky Security Center assets, the fully qualified domain name (FQDN) must be specified for the asset in the system (the "Full device name" field). Otherwise, no response actions can be started.

You can also import events to KUMA and receive information about Kaspersky Endpoint Detection and Response alerts (for more details, see the *Configuring integration with an SIEM system* section of the Kaspersky Anti Targeted Attack Platform online help).

When KUMA is integrated with Kaspersky Endpoint Detection and Response, you can perform the following operations on Kaspersky Endpoint Detection and Response assets that have Kaspersky Endpoint Agent:

- Manage network isolation of assets.
- Manage prevention rules.
- Start applications.

To get instructions on configuring integration for response action management, contact your account manager or Technical Support.

Importing Kaspersky Endpoint Detection and Response events using the kafka connector

When importing events from Kaspersky Endpoint Detection and Response, telemetry is transmitted in clear text and may be intercepted by an intruder.

Kaspersky Endpoint Detection and Response 4.0, 4.1, 5.0, and 5.1 events can be imported to KUMA using a Kafka connector.

Several limitations are applicable to the import of events from Kaspersky Endpoint Detection and Response 4.0 and 4.1:

- Import of events is available if the KATA and KEDR license keys are used in Kaspersky Endpoint Detection and Response.
- Import of events is **not** available if the Sensor component installed on a separate server is used as part of Kaspersky Endpoint Detection and Response.

To import events, perform the actions in Kaspersky Endpoint Detection and Response and in KUMA.

Importing events from Kaspersky Endpoint Detection and Response 4.0 or 4.1

To import Kaspersky Endpoint Detection and Response 4.0 or 4.1 events to KUMA:

In Kaspersky Endpoint Detection and Response:

1. Use SSH or a terminal to log in to the management console of the Central Node server from which you want to export events.
2. When prompted by the system, enter the administrator account name and the password that was set during installation of Kaspersky Endpoint Detection and Response.

   The application component administrator menu is displayed.
3. In the application component administrator menu, select **Technical Support Mode**.
4. Press **Enter**.

   The Technical Support Mode confirmation window opens.
5. Confirm that you want to operate the application in Technical Support Mode. To do so, select **Yes** and press **Enter**.
6. Run the following command:

   ```
   sudo -i
   ```
7. In the `/etc/sysconfig/apt-services` configuration file, in the `KAFKA_PORTS` field, delete the `10000` value.

If Secondary Central Node servers or the Sensor component installed on a separate server are connected to the Central Node server, you need to allow the connection with the server where you modified the configuration file via port 10000.

We do not recommend using this port for any external connections other than KUMA. To restrict connections over port 10000 only for KUMA, run the following command:

```
iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
```

8. In the `/usr/bin/apt-start-sedr-iptables` configuration file, add the `10000` value to the `WEB_PORTS` field, separated by a comma without a space.

9. Run the following command:

```
sudo sh /usr/bin/apt-start-sedr-iptables
```

Preparations for exporting events on the Kaspersky Endpoint Detection and Response side are now complete.

In KUMA:

1. On the KUMA server, add the IP address of the Central Node server in the format `<IP address> centralnode` to one of the following files:

   - `%WINDIR%\System32\drivers\etc\hosts`—for Windows.

   - `/etc/hosts`—for Linux.

2. In the KUMA web interface, create a connector of the Kafka type.

   When creating a connector, specify the following parameters:

   - In the **URL** field, specify `<Central Node server IP address>:10000`.

   - In the **Topic** field, specify `EndpointEnrichedEventsTopic`.

   - In the **Consumer group** field, specify any unique name.

3. In the KUMA web interface, create a collector.

   Use the connector created at the previous step as the transport for the collector. Use "[OOTB] KEDR telemetry" as the normalizer for the collector.

If the collector is successfully created and installed, Kaspersky Endpoint Detection and Response events will be imported into KUMA. You can find and view these events in the events table.

Importing events from Kaspersky Endpoint Detection and Response 5.0 and 5.1

Several limitations apply when importing events from Kaspersky Endpoint Detection and Response 5.0 and 5.1:

- Import of events is available only for the non-high-availability version of Kaspersky Endpoint Detection and Response.
- Import of events is available if the KATA and KEDR license keys are used in Kaspersky Endpoint Detection and Response.
- Import of events is **not** available if the Sensor component installed on a separate server is used as part of Kaspersky Endpoint Detection and Response.

To import Kaspersky Endpoint Detection and Response 5.0 or 5.1 events to KUMA:

In Kaspersky Endpoint Detection and Response:

1. Use SSH or a terminal to log in to the management console of the Central Node server from which you want to export events.
2. When prompted by the system, enter the administrator account name and the password that was set during installation of Kaspersky Endpoint Detection and Response.

   The application component administrator menu is displayed.
3. In the application component administrator menu, select **Technical Support Mode**.
4. Press **Enter**.

   The Technical Support Mode confirmation window opens.
5. Confirm that you want to operate the application in Technical Support Mode. To do so, select **Yes** and press **Enter**.
6. In the `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` configuration file, specify the additional port `10000` for the `WEB_PORTS` constant:

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

   You do not need to perform this step for Kaspersky Endpoint Detection and Response 5.1 because the port is specified by default.
7. Run the following commands:

   ```
   kata-firewall stop
   kata-firewall start --cluster-subnet <mask>
   ```

   where:

   <mask> is the network mask for addressing cluster servers.

Preparations for exporting events on the Kaspersky Endpoint Detection and Response side are now complete.

In KUMA:

1. On the KUMA server, add the IP address of the Central Node server in the format `<IP address> kafka.services.external.dyn.kata` to one of the following files:

   - `%WINDIR%\System32\drivers\etc\hosts`—for Windows.
   - `/etc/hosts`—for Linux.

2. In the KUMA web interface, create a connector of the Kafka type.

   When creating a connector, specify the following parameters:

   - In the **URL** field, specify `<Central Node server IP address>:10000`.
   - In the **Topic** field, specify `EndpointEnrichedEventsTopic`.
   - In the **Consumer group** field, specify any unique name.

3. In the KUMA web interface, create a collector.

   Use the connector created at the previous step as the transport for the collector. It is recommended to use the **[OOTB] KEDR telemetry** normalizer as the normalizer for the collector.

If the collector is successfully created and installed, Kaspersky Endpoint Detection and Response events will be imported into KUMA. You can find and view these events in the events table.

Importing Kaspersky Endpoint Detection and Response events using the kata/edr connector

To use the kata/edr connector to import events of Kaspersky Endpoint Detection and Response 5.1 or earlier from hosts:

1. Configure event receipt on the KUMA side. To do this, in KUMA, create and install a collector with the 'kata/edr' connector or edit an existing collector, then save the modified settings and restart the collector.

2. On the KEDR side, accept the authorization request from KUMA to begin receiving events in KUMA.

As a result, the integration is configured and KEDR events start arriving in KUMA.

Creating a collector for receiving events from KEDR

To create a collector for receiving events from KEDR:

1. In KUMA → **Resources** → **Collectors**, select **Add collector**.

2. This opens the **Create collector** window; in that window, at step 1 **Connect event sources**, specify an arbitrary **Collector name** and in the drop-down list, select the appropriate **Tenant**.

3. At step 2 **Transport**:

   1. On the **Basic settings** tab:

      a. In the **Connector** field, select **Create** or start typing the name of the connector if you want to use a previously created connector.

      b. In the **Connector type** drop-down list, select the **kata/edr** connector. After you select the kata/edr connector type, more fields to fill in are displayed.

      c. In the **URL** field, specify the address for connecting to the KEDR server in the following `<name or IP address of the host>:<connection port, 443 by default>` format. If the KEDR solution is deployed in a cluster, you can click **Add** to add all nodes. KUMA will connect to each specified node in sequence. If the KEDR solution is installed in a distributed configuration, on the KUMA side, you must configure a separate collector for each KEDR server.

      d. In the **Secret** field, select **Create** to create a new secret. This opens the **Create secret** window; in that window, specify the **Name** and click **Generate and download a certificate and private encryption key**.

         As a result, the certificate.zip archive is downloaded to the browser's Downloads folder; the archive contains the 'key.pem' key file and the 'cert.pem' certificate file. Extract the archive. Click **Upload certificate** and select the cert.pem file. Click **Upload private key** and select the key.pem file. Click **Create**; the secret is added to the **Secret** drop-down list and automatically selected.

         You can also select the created secret from the **Secret** list. KUMA uses the selected secret to connect to KEDR.

      e. The **External ID** field contains the ID for external systems. This ID is displayed in the KEDR web interface when authorizing the KUMA server. KUMA generates an ID automatically and the **External ID** field is automatically pre-populated.

   2. On the **Advanced settings** tab:

      a. To get detailed information in the collector log, move the **Debug** toggle switch to the enabled position.

      b. If necessary, in the **Character encoding** field, select the encoding of the source data to be converted to UTF-8. We only recommend configuring a conversion if you find invalid characters in the fields of the normalized event. By default, no value is selected.

      c. Specify the maximum **Number of events** per one request to KEDR. The default value is 0, which means that KUMA uses the value specified on the KEDR server. For details, refer to KATA Help. You can specify an arbitrary value that must not exceed the value on the KEDR side. If the value you specify exceeds the value of the **Maximum number of events** setting specified on the KEDR server, the KUMA collector log displays the *Bad Request: max_events N is greater than the allowed value* error.

      d. Fill in the **Events fetch timeout** field to receive events after a specified period of time. The default value is 0. This means that the default value of the KEDR server is applied. For details, please refer to KATA Help. This field specifies the time after which the KEDR server must send events to KUMA. The KEDR server uses two parameters: the maximum number of events and the events fetch timeout. Events are sent when the specified number of events is collected or the configured time elapses, whichever happens first. If the specified time has elapsed, but the specified number of events has not been collected, the KEDR server sends the events that it already has, without waiting for more.

e. In the **Client timeout** field, specify how long KUMA must wait for a response from the KEDR server, in seconds. Default value: 1,800 s; displayed as 0. The client-side limit is specified in the **Client timeout** field. The **Client timeout** must be greater than the **Events fetch timeout** of the server to wait for the server's response without interrupting the current event collection task with a new request. If the response from the KEDR server does not arrive in the end, KUMA repeats the request.

f. In the **KEDRQL filter** field, specify the conditions for filtering the request. As a result, pre-filtered events are received from KEDR. For details about available filter fields, please refer to the KATA Help.

4. At step 3 **Parsing**, click **Add event parsing** and select [OOTB] KEDR telemetry in the **Basic event parsing** window.

5. To finish creating the collector in the web interface, click **Create and save service**. Then copy the collector installation command from the web interface and run this installation command on the command line on the server where you want to install the collector.

   If you were editing an existing collector, click **Save and restart services**.

As a result, the collector is created and is ready to send requests; the collector is displayed in the **Resources** → **Active services** section with the yellow status until KEDR accepts an authorization request from KUMA.

Authorizing KUMA on the KEDR side

After the collector is created in KUMA, for requests from KUMA to start arriving to KEDR, the KUMA authorization request must be accepted on the KEDR side. With the authorization request accepted, the KUMA collector automatically sends scheduled requests to KEDR and waits for a response. While waiting, the status of the collector is yellow, and after receiving the first response to a request, the status of the collector turns green.

As a result, the integration is configured and you can view events arriving from KEDR in the KUMA → **Events** section.

The initial request fetches part of the historical events that had occurred before the integration was configured. Current events begin arriving after all of the historical events. If you change the value of the **URL** setting or the **External ID** of an existing collector, KEDR treats the next request as an initial request, and after starting the KUMA collector with the modified settings, you will receive part of the historical events all over again. If you do not want to receive historical events, go to the settings of the relevant collector, configure the mapping of the KEDR and KUMA `timestamp` fields in the normalizer, and specify a filter by `timestamp` at the 'Event filtering' step of the Collector Installation Wizard — the `timestamp` of the event must be greater than the `timestamp` when the collector is started.

Possible errors and solutions

If in the collector log, you see the *Conflict: An external system with the following ip and certificate digest already exists. Either delete it or provide a new certificate* error, create a new secret with a new certificate in the connector of the collector.

If in the collector log, you see the *Continuation token not found* error in response to an event request, create a new connector, attach it to the collector and restart the collector; alternatively, create a new secret with a new certificate in the connector of the collector. If you do not want to receive events generated before the error occurred, configure a Timestamp filter in the collector.

Configuring the display of a link to a Kaspersky Endpoint Detection and Response detection in KUMA event details

You can configure the creation of an alert or each received Kaspersky Endpoint Detection and Response detection. You can configure the display of a link to a Kaspersky Endpoint Detection and Response detection in KUMA alert information.

> You can configure the display of a detection link if you use only one Central Node server in Kaspersky Endpoint Detection and Response. If Kaspersky Endpoint Detection and Response is used in a distributed solution mode, it is impossible to configure the display of the links to Kaspersky Endpoint Detection and Response detections in KUMA.

To configure the display of a link to a detection in KUMA alert details, you need to complete steps in the Kaspersky Endpoint Detection and Response web interface and KUMA.

In the Kaspersky Endpoint Detection and Response web interface, you need to configure the integration of the application with KUMA as a SIEM system. For details on configuring integration, refer to the *Kaspersky Anti Targeted Attack Platform* documentation, *Configuring integration with a SIEM system* section.

Configuring the display of a link in the KUMA web interface includes the following steps:

1. Adding an asset that contains information about the Kaspersky Endpoint Detection and Response Central Node server from which you want to receive detections, and assigning a category to that asset.

2. Creating a correlation rule.

3. Creating a correlator.

4. Adding a collector, taking into account the following:

   - At the **Transport** step, specify the connector type (TCP or UDP) and the connection port (must be the same as the port configured in the SIEM connection settings in Kaspersky Anti Targeted Attack Platform).

   - At the **Parsing** step, when selecting a normalizer, you need to specify mappings for KEDR event fields or select the `[OOTB] KATA` normalizer.

   - After adding the correlator, in the collector, you need to specify a destination pointing to the correlator.

You can use a pre-configured correlation rule. In this case configuring the display of a link in the KUMA web interface includes the following steps:

1. Creating a correlator.

   Select the `[OOTB] KATA Alert` correlation rule.

2. Adding an asset that contains information about the Kaspersky Endpoint Detection and Response Central Node server from which you want to receive detections and assigning a category `KATA standAlone` to that asset.

Step 1. Adding an asset and assigning a category to it

First, you need to create a category that will be assigned to the asset being added.

To add a category:

1. In the web interface, open the **Assets** section.
2. On the **All assets** tab, expand the list of tenant categories by doing one of the following:
   - Under **All tenants**, click the menu icon (•••) and select **Expand all**.
   - In the **All tenants** object tree, click the arrow icon (▸) next to the name of the tenant.
3. Select a category or subcategory and do one of the following:
4. Click the add icon (+).
5. Click the menu icon (⋮) and select **Add subcategory**.
   The **Add category** sidebar is displayed in the right part of the web interface window.
6. Define the category settings:
   a. In the **Name** field, enter the name of the category.
   b. In the **Parent** drop-down list, select categories from the tree of categories.
   c. In the **Tenant** drop-down list, select a tenant if it is not automatically specified.
   d. In the **Categorization kind** drop-down list, select how the category will be populated with assets. Depending on your selection, you may need to specify additional settings:
      - **Manually**—assets can only be manually linked to a category.
      - **Active**—assets will be assigned to a category at regular intervals if they satisfy the defined filter.

        How to configure a filter

        1. In the **Repeat categorization every** drop-down list, specify how often assets will be linked to a category. You can select values ranging from once per hour to once per 24 hours.

           You can forcibly start categorization by selecting **Start categorization** in the category context menu.
        2. Under **Conditions**, specify the filter for matching assets to attach to an asset category.

           You can add conditions by clicking the **Add condition** buttons. Groups of conditions can be added by using the **Add group** buttons. Group operators can be switched between **AND**, **OR**, and **NOT** values.

           Categorization filter operands and operators

Operand	Operators	Comment
Build number	=, ilike	
OS	=, ilike	The **ilike** operator makes the search case-insensitive.
IP address	inSubnet, inRange	The IP address is indicated in CIDR notation (for example: 192.168.0.0/24). When the inRange operator is selected, you can indicate only addresses from private ranges of IP addresses (for example: 10.0.0.0–10.255.255.255). Both addresses must be in the same range.
FQDN	=, ilike	The **ilike** operator makes the search case-insensitive.
CVE	=, in	The **in** operator lets you specify an array of CVE (Common Vulnerabilities and Exposures) IDs, for example, `CVE-2017-0143`.

CVSS	>, >=, =, <=,<	Severity level of CVE vulnerabilities on the asset. The CVSS parameter takes values from 0 to 10. Not applicable to vulnerabilities from Kaspersky Security Center.

CVE count	>, >=, =, <=, <	The number of unique vulnerabilities with the CVE attribute for the asset. Vulnerabilities without CVEs do not count towards this figure.
		For categorization by the number of CVEs of a certain severity level, you can use a combined condition. For example:
		`CVE count >= 1`
		`AND`
		`CVSS >= 6.5`

Software	=, ilike	Categorization by software installed on the asset. The **ilike** operator makes the search case-insensitive.
Software version	=, ilike, in	Categorization by version (build) number of the software installed on the asset. The **ilike** operator makes the search case-insensitive.
CII	in	More than one value can be selected.
KSC group	=, ilike	Categorization by the name of the Kaspersky Security Center administration group in which the asset is placed.
Anti-virus databases last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is current at the time when categorization is started.
Last update of the information	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Protection last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
System last started	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
KSC extended status	in	Extended status of the device. More than one value can be selected.

Real-time protection status	=	Status of Kaspersky applications installed on the managed device.
Encryption status	=	
Spam protection status	=	
Anti-virus protection status of mail servers	=	
Data Leakage Prevention status	=	
KSC extended status ID	=	
Endpoint Sensor status	=	
Last visible	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Score ML	>,>=,=,<=,<	Categorization by asset score assigned by AI services.
Status	=, in	Categorization by predefined asset statuses assigned by AI services.
Custom asset field	=, ilike	Categorization by values of custom asset fields.

Using time values

Some conditions, for example, **Anti-virus databases last updated** or **System last started**, use date and time as the operand value. For these conditions, you can use an exact date and time or a relative period.

To specify a date and time value:

1. Select an operand, an operator and click the date field.

2. Do one of the following:

   - Select the exact date in the calendar.

     By default, the current time is automatically added to the selected date, with millisecond precision. Changing the date in the calendar does not change the specified time. The date and time are displayed in the time zone of the browser. If necessary, you can edit the date and time in the field.

   - In the **Relative period** list, select a relative period.

     The period is calculated relative to the start time of the current categorization and takes into account asset information that is up-to-date at that moment. For example, for the condition **Anti-virus databases last updated**, you can select **1 hour** and the **>=** operator to periodically link to the category those assets for which the anti-virus databases have not been updated for more than 1 hour before the start of categorization.

   - In the date and time field, enter a value manually.

You can enter an exact date and time in the **DD.MM.YYYY HH:mm:ss.SSS** format for the Russian localization and **YYYY-MM-DD HH:mm:ss.SSS** for the English localization or a relative period as a formula. You can also combine these methods if necessary.

If you do not specify milliseconds when entering the exact date, 000 is substituted automatically.

In the relative period formulas, you can use the **now** parameter for the current date and time and the interval parameterization language: **+**, **-**, **/** (rounding to the nearest), as well as time units: **y** (year), **M** (month), **w** (week), **d** (day), **h** (hour), **m** (minute), **s** (second).

For example, for the **Information last updated** condition, you can specify the value **now-2d** with the operator **>=** operator and the value **now-1d** with the **>=** operator to regularly link assets to the category if those assets had information updated during the day before the categorization was started; alternatively, you can specify the value **now/w** with the **<=** operator to regularly link assets to the category if those assets had information updated between the beginning of the first day of the current week (00:00:00:000 UTC) and **now**.

KUMA stores time values in UTC, but in the user interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the period, the category will cover assets from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the date and time field by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want the categorization to cover the **Yesterday** period, you need to change the value to **now-1d/d-3h**. If you want the categorization to cover the **Today** period, change the value to **now/d-3h**.

3. Use the **Test conditions** button to make sure that the specified filter is correct. When you click the button, the **Assets for given conditions** window containing a list of assets that satisfy the search conditions will be displayed.

- **Reactive**—the category will be filled with assets by using correlation rules.

e. If required, define the values for the following settings:

- Assign a severity to the category in the **Severity** drop-down list.

  The specified severity is assigned to correlation events and alerts associated with the asset.

- Add a description for the category in the **Description** field.

7. Click the **Save** button.

To add an asset:

1. In the KUMA web interface, select the **Assets** section.

2. Click the **Add asset** button.

   The **Add asset** details area opens in the right part of the window.

3. Define the following asset parameters:

   a. In the **Asset name** field, enter a name for the asset.

   b. In the **Tenant** drop-down list, select the tenant that will own the asset.

c. In the **IP address** field, specify the IP address of the Kaspersky Endpoint Detection and Response Central Node server from which you want to receive detections. If necessary, you can add one or more server IP addresses.

d. If required, define the values for the following fields:

- In the **FQDN** field, specify the Fully Qualified Domain Name of the Kaspersky Endpoint Detection and Response server.
- In the **MAC address** field, specify the MAC address of the Central Node Kaspersky Endpoint Detection and Response Central Node server.
- In the **Owner** field, define the name of the asset owner.
- In the **Categories** field, select the category of the tenant.
- In the **CII categories** drop-down list, select the critical information infrastructure category of the resource.

4. If necessary, under **Software**, specify the name and version of the operating system.

5. If necessary, in the **Hardware info** section, specify the following parameters of the hardware:

- Name, core count, and clock rate of the CPU in MHz. If necessary, you can click the **Add CPU** button specify more CPUs.
- Free disk space and the total size of the disk in bytes. If necessary, you can click the **Add disk** button specify more disks to be used.
- Name, vendor, and driver version of the network adapter. If necessary, you can click the **Add network card** button to specify more network adapters.
- The clock rate of the RAM in MHz and the total amount of RAM in bytes.

6. Click the **Save** button.

Step 2. Adding a correlation rule

You can create a correlation rule or use the ready-made `[OOTB] KATA Alert` rule.

To add a correlation rule:

1. In the KUMA web interface, select the **Resources** section.

2. Under **Resources**, select **Correlation rules** and click the **Add** button.

3. On the **General** tab, specify the following settings:

a. In the **Name** field, define the rule name.

b. In the **Tenant** drop-down list, select a tenant.

c. In the **Type** drop-down list, select **simple**.

d. In the **Tags** drop-down list, select one or more tags to identify the rule.

e. In the **Propagated fields** field, add the following fields: **DeviceProduct**, **DeviceAddress**, **EventOutcome**, **SourceAssetID**, **DeviceAssetID**

f. If required, define the values for the following fields:

- In the **Rate limit** field, define the maximum number of times per second that the rule will be triggered.
- In the **Severity** field, define the severity of alerts and correlation events that will be created as a result of the rule being triggered.
- In the **Description** field, provide any additional information.
- In the **MITRE Techniques** drop-down list, select the applicable MITRE ATT&CK techniques.

4. On the **Selectors** → **Settings** tab, specify the following filter settings:

a. In the **Filter** drop-down list, select **Create new**.

b. Click **Add group**.

c. In the operator field for the group you added, select **AND**.

d. Add a condition for filtering by KATA value:

1. In the **Conditions** field, click the **Add condition** button.
2. In the condition field, select **If**.
3. In the **Left operand** field, select **Event fields**.
4. In the **Event fields** field, select **DeviceProduct**.
5. In the **Operator** field, select =.
6. In the **Right operand** field, select **Constant**.
7. In the **value** field, enter KATA.

e. Add a category filter condition:

1. In the **Conditions** field, click the **Add condition** button.
2. In the condition field, select **If**.
3. In the **Left operand** field, select **Event fields**.
4. In the **Event fields** field, select **DeviceAssetID**.
5. In the **Operator** field, select **inCategory**.
6. In the **Right operand** field, select **Constant**.
7. Click the **Builder** button.

8. Select the category in which you placed the Kaspersky Endpoint Detection and Response Central Node server asset.

9. Click the **Save** button.

f. In the **Conditions** field, click the **Add group** button.

g. In the operator field for the group you added, select **OR**.

h. Add a condition for filtering by event class identifier:

1. In the **Conditions** field, click the **Add condition** button.

2. In the condition field, select **If**.

3. In the **Left operand** field, select **Event fields**.

4. In the **Event fields** field, select **DeviceEventClassID**.

5. In the **Operator** field, select =.

6. In the **Right operand** field, select **Constant**.

7. In the **Value** field, enter **taaScanning**.

i. Repeat steps 1 through 7 under (h) for each of the following event class IDs:

- file_web
- file_mail
- file_endpoint
- file_external
- ids
- url_web
- url_mail
- dns
- iocScanningEP
- yaraScanningEP

5. On the **Actions** tab, specify the following settings:

a. Select the **Output** check box.

b. In the **Enrichment** section, click the **Add enrichment** button.

c. In the **Source kind** drop-down list, select **Template**.

d. In the **Template** field, enter:

```
https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}
```

e. In the **Target field** drop-down list, select **DeviceExternalID**.

> If you want the **DeviceExternalID** value to be displayed as a link in the event properties, make sure that the **Template** field for the `DeviceAddress` parameter contains a URL or fully qualified domain name followed by the "/" character, for example: `https://example.com:8443/` or `https://example.com/`.

f. If necessary, turn on the **Debug** toggle switch to log information related to the operation of the resource.

6. Click the **Save** button.

Step 3. Creating a correlator

Start the Correlator Installation Wizard. At step 3 of the wizard, select the correlation rule that you added while following these steps.

After the correlator is created, a link to these detections will be displayed in the details of alerts created when receiving detections from Kaspersky Endpoint Detection and Response. The link is displayed in the correlation event details (**Related events** section), in the **DeviceExternalID** field.

> If you want the FQDN of the Kaspersky Endpoint Detection and Response Central Node server to be displayed in the DeviceHostName field, in the detection details, you need to create a DNS record for the server and create a DNS enrichment rule at `step 4` of the wizard.

Integration with Kaspersky CyberTrace

Kaspersky CyberTrace (hereinafter CyberTrace) is a tool that integrates threat data streams with SIEM solutions. It provides users with instant access to analytics data, increasing their awareness of security decisions.

You can integrate CyberTrace with KUMA in one of the following ways:

- Integrate CyberTrace indicator search feature to enrich KUMA events with information from CyberTrace data streams.
- Integrate the entire CyberTrace web interface into KUMA to get full access to CyberTrace.

> Integration with the CyberTrace web interface requires the CyberTrace TIP Enterprise license.

You can also configure retroscan and event enrichment using CyberTrace. This allows KUMA to get notifications for events in which threat indicators had not been initially detected, but were discovered later after an update of the feeds. This can improve the accuracy of threat detection based on previously logged events.

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

Integrating CyberTrace indicator search

To integrate CyberTrace indicator search:

1. Configure CyberTrace to receive and process KUMA requests.

   You can configure the integration with KUMA immediately after installing CyberTrace in the Quick Start Wizard or later in the CyberTrace web interface.

2. Create an event enrichment rule in KUMA.

   In the enrichment rule, you can specify which data from CyberTrace you want to enrich the event with. We recommend selecting cybertrace-http as the source kind.

3. Create a collector to receive events that you want to enrich with CyberTrace data.

4. Link the enrichment rule to the collector.

5. Save and create the service:

   - If you linked the rule to a new collector, click **Save and create**, copy the collector ID in the opened window and use the copied ID to install the collector on the server using the command line interface.

   - If you linked the rule to an existing collector, click **Save and restart services** to apply the settings.

   The configuration of the integration of CyberTrace indicator search is complete and KUMA events will be enriched with CyberTrace data.

Example of testing data enrichment from CyberTrace

By default, KUMA does not test the connection with CyberTrace.

If you want to test the integration with CyberTrace and make sure that event enrichment is working, you can follow the steps of the following example or adapt the example to your situation. The example shows an integration test, which performs enrichment and shows that the event contains the specified test URL.

To run the test:

1. Create a test enrichment rule with the following parameters:

   - **Name**: Test CT enrichment.
   - **Tenant**: Shared.
   - **Data source type**: cybertrace-http.
   - **URL**: <URL of the cybertrace server to which you want to send requests>:9999.
   - **Mapping**: KUMA field: RequestURL; CyberTrace indicator: url.
   - **Debugging**: Enabled.

2. Create a test collector with the following parameters:

   At step **2 Transport**, specify the http connector.

   At step **3 Parsing**, specify the normalizer and select the json parsing method, set the mapping of the `RequestUrl` – `RequestUrl` fields.

   At step **6 Enrichment**, specify the 'Test CT enrichment' rule.

   At step **7 Routing**, specify the storage where events must be sent.

3. Click **Create and save service**.

   A complete command for installing the collector is displayed in the window.

4. Click **Copy** to copy the command to the clipboard and run the command on the command line. Wait for the command to complete, return to the KUMA web interface, and click **Save collector**.

   A test collector is created and the test enrichment rule is linked to the collector.

5. Use the command line interface to send a request to the collector, which will trigger an event, which will then be enriched with the test URL `http://fakess123bn.nu`.

   Example

   ```
   curl --request POST \  --url http://<ID of the host where the collector is installed>:<port of the collector>/input \  --header 'Content-Type: application/json' \  --data '{"RequestUrl":"http://fakess123bn.nu"}'
   ```

6. Go to the KUMA **Events** section and run the following query to filter event output and find the enriched event:

   ```
   SELECT * FROM `events` WHERE RequestUrl = 'http://fakess123bn.nu' ORDER BY Timestamp DESC LIMIT 250
   ```

Enrichment completed successfully. The event now has a **RequestURL** field with the `http://fakess123bn.nu` value, as well as a TI indicator and indicator category with CyberTrace data.

If the test did not result in enrichment, for example, if the TI indicator is missing, we recommend to do the following:

1. Check the settings of the collector and enrichment rules.

2. Download the collector logs using the following command and look for errors in the logs:

```
tail -f /opt/kaspersky/kuma/collector/<collector ID>/log/collector
```

Configuring CyberTrace to receive and process requests

You can configure CyberTrace to receive and process requests from KUMA immediately after its installation in the Quick Start Wizard or later in the application web interface.

To configure CyberTrace to receive and process requests in the Quick Start Wizard:

1. Wait for the CyberTrace Quick Start Wizard to start after the application is installed.

   The wizard starts at step 1, **Welcome to Kaspersky CyberTrace**. You can go to the next step of the wizard by clicking **Next**.

2. At step 2, **Proxy settings**, if your organization uses a proxy server, enter its connection settings. If your organization does not use a proxy server, leave all fields blank.

3. At step 3, **Licensing settings**, select the method for adding a license key for CyberTrace: an activation code or a license key file. Depending on the selected method, specify the activation code or upload a license key file.

4. At step 4, **Service settings**, keep default settings.

5. At step 5, **Data management settings**:

   a. In the **SIEM system** drop-down list, select **KUMA**.

   b. Under **Listen on**, select the **IP and port** option.

   c. In the **IP address** field, enter `0.0.0.0`.

   d. In the **Port** field, enter the port to listen on for events. The default port is `9999`.

   e. Under **Send detection alerts**, in the **IP address** field, enter `127.0.0.1`, and in the **Port** field, enter `9998`.

   Leave the default values for everything else.

6. At step 6, **Certificate settings**, select **Commercial certificate** and add a certificate that allows you to download data feeds from update servers.

7. At step 7, **Feeds settings**, keep default settings.

CyberTrace is configured.

To configure CyberTrace to receive and process requests in the application web interface:

1. In the window of the CyberTrace web interface, switch **Data management** mode: in the left menu, select **System**, and then in the displayed menu, select **General**.

2. Select the **Settings** → **General** section.

3. Under **Listen on**:

   a. Select **IP and port**.

   b. In the **IP address** field, enter `0.0.0.0`.

   c. In the **Port** field, enter the port to listen on for events. The default port is `9999`.

4. Select the **Settings** → **Service alerts** section.

5. In the **Service alert format** field, enter `%Date% alert=%Alert%%RecordContext%`.

6. In the **Records context format** field, enter `|%ParamName%=%ParamValue%`.

7. Select the **Settings** → **Detection alerts** section.

8. In the **Alert format** field, enter `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.

9. On the **Context** tab, in the **Actionable fields** field, enter `%ParamName%:%ParamValue%`.

10. Switch to the **System management** mode: in the left menu, select **General**, then in the displayed menu, select **System**.

11. Select the **Settings** → **Service** section.

12. Under **Web interface**, in the **IP address or host name**, enter `127.0.0.1`.

13. In the upper toolbar, click **Restart service**.

14. Restart the CyberTrace server.

CyberTrace is configured.

Creating event Enrichment rules

To create event enrichment rules:

1. In the KUMA web interface, open **Resources** → **Enrichment rules**.

   The list of available enrichment rules will be displayed.

2. Click the **Add** button to create the new rule.

3. This opens a window; in that window, specify the enrichment rule settings:

   a. In the **Name** field, enter a unique name for the rule. The name must contain 1 to 128 Unicode characters.

   b. In the **Tenant** drop-down list, select the tenant that will own this resource.

   c. In the **Source kind** drop-down list, select **cybertrace-http**.

   d. Specify the **URL** of the CyberTrace server to which you want to connect. For example, *example.domain.com:443*.

   e. In the **Secret** field, select or create a secret for the connection.

   f. In the **Key fields** drop-down list, select the event fields used for enrichment of events with data from CyberTrace.

   g. If necessary, use the **Timeout** field to specify the maximum number of connections to the CyberTrace server that can be simultaneously established by KUMA. By default, this value is equal to the number of vCPUs of the KUMA Core server.

   h. In the **RPS** field, enter the number of requests to the CyberTrace server per second that KUMA can make. The default value is `1000`.

   i. In the **Timeout** field, specify the maximum number of seconds KUMA should wait for a response from the CyberTrace server. Until a response is received or the time expires, the event is not sent to the Correlator. If a response is received before the timeout, it is added to the `TI` field of the event and the event processing continues.

   j. In the **Maximum number of events in enrichment queue** field, specify the maximum number of events stored in the enrichment queue for re-sending. The default setting is 1000000.

   k. Use the **Major version of Cybertrace** toggle switch to specify the CyberTrace version. Possible values: <5 and ≥ 5. If you select version ≥ 5, requests are executed in the General tenant in CyberTrace and use the new API version corresponding to CyberTrace 5.0 and higher; CyberTrace can also display statistics and retrospective analysis information for enrichment requests from KUMA that are made over HTTP. If you select <5, requests use the Kaspersky CyberTrace 4.x API. The default setting is <5.

   l. Use the **Debug** toggle switch to indicate whether or not to enable logging of service operations. Logging is disabled by default.

   m. In the **Tags** drop-down list, select the tags for the event enrichment rule.

   n. If necessary, in the **Description** field, add up to 4,000 Unicode characters describing the resource.

   o. Under **Filter parameters**, you can specify conditions to identify events that will be processed using the enrichment rule. You can select an existing filter from the **Filter** drop-down list or **Create** a new filter.

      Creating a filter in resources

      All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

To create a filter:

1. In the **Filter** drop-down list, select **Create new**.

2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

4. Select the filter creation mode: **Constructor** or **Code**.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

5. If you selected the **Constructor** option, do the following:

   a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

   b. Click the **Add condition** button.

   c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

   d. From the drop-down lists, select operands and filter operators.

      Operands of filters

      - **Event fields** specify the field of the event that you need to use as a filter operand.

      - **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

        If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.

      - **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:

        - **dictionary** (required) is the dictionary that you want to use.

        - **key fields** (required) are event fields that are used to generate the key of the dictionary value.

      - In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:

        - **context table name** (required) is the context table that you want to use.

        - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.

- **field** is the name of the context table field from which you want to get the value of the operand.
- **index** is the index of the list field of the table from which you want to get the value of the operand.

- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.

- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.

- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.

- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.

- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.

- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.

- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.

- **inContextTable** checks for the presence of the entry in the specified context table.

- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ×.

8. Click **Save**.

4. Click **Create**.

A new enrichment rule will be created.

CyberTrace indicator search integration is now configured. You can now add the created enrichment rule to a collector. To apply the new settings, you need to restart KUMA collectors.

If any of the CyberTrace fields in the events details area contains "[{" or "}]" values, it means that information from CyberTrace data feed was processed incorrectly and it's possible that some of the data is not displayed. You can get all information from a data feed by copying value of the **TI indicator** event field from KUMA and searching for it in CyberTrace in the **Indicators** section. All information about the found indicator is displayed on the **Indicator details** page.

Integrating CyberTrace interface

You can integrate the Kaspersky CyberTrace web interface into the KUMA web interface. When this integration is enabled, the KUMA web interface includes a **CyberTrace** section that provides access to the CyberTrace web interface.

After you integrate the Kaspersky CyberTrace web interface, you will need to configure the receipt of Kaspersky CyberTrace events.

To integrate the CyberTrace web interface in KUMA:

1. In the KUMA web interface, open the **Resources** → **Resources** → **Secrets**.

   The list of available secrets is displayed.

2. Click the **Add** button to create a new secret. This resource is used to store credentials of the CyberTrace server.

   This opens the incident creation window.

3. Enter information about the secret:

   a. In the **Name** field, choose a name for the added secret. The name must contain 1 to 128 Unicode characters.

   b. In the **Tenant** drop-down list, select the tenant that will own this resource.

   c. In the **Type** drop-down list, select **credentials**.

   d. In the **User** and **Password** fields, enter credentials for your CyberTrace server.

   e. If necessary, select the tags for the secret from the **Tags** drop-down list.

   f. If necessary, in the **Description** field, add up to 4,000 Unicode characters describing the resource.

4. Click **Create**.

   The CyberTrace server credentials are now saved and can be used in other KUMA resources.

5. In the KUMA web interface, open **Settings** → **Integrations** → **Kaspersky CyberTrace**.

   The window with CyberTrace integration parameters opens.

6. Manage the settings as follows:

   - Enable the **State** toggle switch if you want to enable the integration of the CyberTrace web interface into the KUMA web interface.

   - **Host** (required)—enter the address of the CyberTrace server.

   - **Port** (required)—enter the port of the CyberTrace server; the default port for managing the web interface is 443.

   - In the **Secret** drop-down list, select a previously created secret of the **credentials** type.

   - In the **Allow hosts** drop-down list, select the hosts that support the CORS technology.

   - In the **Major version of CyberTrace** field, select the CyberTrace version. Possible values: **<5**, **≥ 5.0**. If version **≥ 5.0** is selected, requests are executed in the General tenant in CyberTrace and use the new version of the API provided by Kaspersky CyberTrace 5.0 and later. If you select **<5**, requests use the Kaspersky CyberTrace 4.x API. The default value is **<5**.

7. You can configure access to the CyberTrace web interface in the following ways:

   - Use hostname or IP when logging into the KUMA web interface.

     To do this, in the Allow hosts section, click Add host and in the field that is displayed, enter the IP or hostname of the device

     on which the KUMA web interface is deployed.

   - Use the FQDN when logging into the KUMA web interface.

     If you are using the Mozilla Firefox browser to manage the solution web interface, the CyberTrace section may fail to display data. In this case, configure the data display (see the instructions below).

8. Click **Save**.

The Kaspersky CyberTrace web interface is integrated with KUMA. The **CyberTrace** section is displayed in the KUMA web interface

Displaying data in the CyberTrace section

To configure the data display in the CyberTrace section when using the FQDN to log in to KUMA in Mozilla Firefox:

1. Clear your browser cache.

2. In the browser's address bar, enter the FQDN of the KUMA web interface with port number 7222 as follows: https://kuma.example.com:7222.

   A window will open to warn you of a potential security threat.

3. Click the **Details** button.

4. In the lower part of the window, click the **Accept risk and continue** button.

   An exclusion will be created for the URL of the KUMA web interface.

5. In the browser's address bar, enter the URL of the KUMA web interface with port number 7220.

6. Go to the **CyberTrace** section.

   Data will be displayed in this section.

Updating CyberTrace deny list (Internal TI)

When the CyberTrace web interface is integrated into the KUMA web interface, you can update the CyberTrace denylist or **Internal TI** with information from KUMA events.

To update CyberTrace Internal TI:

1. Open the event details area from the events table, Alert window, or correlation event window and click the link on a domain, web address, IP address, or file hash.

   The context menu opens.

2. Select **Add to Internal TI of CyberTrace**.

   A confirmation window opens.

3. If you want to confirm your actions and update the **Internal TI** with data from KUMA events, click **Yes**.

   The selected object is now added to the CyberTrace denylist.

Configuring event enrichment and retroscan

Integration of KUMA with Kaspersky CyberTrace (hereinafter referred to as CyberTrace) version 5.0 and later allows enriching events with information about indicators of compromise (IoC) and retrospectively scanning events. Retroscan helps detect indicators that had not been detected at the time of initial enrichment, but appeared later in updated CyberTrace feeds. Retroscan can be used in the following cases:

- The incident has already occurred, but its indicators became known only after the feeds were updated.
- You want to rescan saved events for new threats.

To set up data enrichment and retroscan:

1. Perform the initial configuration in KUMA by following these steps:

   a. Configure CyberTrace integration.

   b. Create two collectors to receive events that you want to enrich with CyberTrace data.

      - To get notifications from CyberTrace about the triggering of indicators, create a collector in which a connector of the **tcp** type is used as the transport, and the normalizer is **[OOTB] CyberTrace**.

      - To configure event enrichment, create a collector with the following parameters:

        - Select any connector (for example, **http**) as the transport.

        - You can choose any normalization method (for example, **json**) with the mapping of the following fields: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.

        - As the enrichment, create an event enrichment rule in which the data source type is **cybertrace-http**, the CyberTrace version is **≥ 5.0**, and the following normalizer fields are selected in the **Key fields** drop-down list: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.

2. To configure retroscan in the CyberTrace web interface, follow these steps:

   a. In the **General** → **General** section, enable **API lookup** to save detected indicators and collect statistics a public API request is used.

   b. On the **General** → **Retroscan** page, enable retrospective scan, then select the **Regular expressions** and enable the sources and regular expressions that you want to use for retrospective scan.

   c. In the **General** → **General** section, under **Detection alerts**, specify the IP address and port that CyberTrace will use to send alerts about the detection of indicators of compromise.

   d. In the **General** → **General** section, under **Service alerts**, configure CyberTrace service notifications (for example, notifications about the retroscan task finishing or license key replacement) by specifying the IP address of the collector and the port of the KUMA TCP connector.

   For more information on configuring retroscan, see the *Kaspersky CyberTrace Help*.

Event processing stages during retroscan

Retroscan allows detecting indicators of compromise that had not been known when an event was received, but became available later after an update of Kaspersky CyberTrace feeds.

The retroscan algorithm comprises the following steps:

1 Sending an event to CyberTrace

An event containing indicators is received at the CyberTrace collector. When received, these indicators may not be present in active feeds.

Example event

```
{
"SourceHostName": "45.54.64.52",
"DestinationHostName": "geardox.site",
"Message": "5BA7335AD847E5ED6211FB27094B9855",
"DeviceHostName": "test.domain.ru",
"DeviceAddress": "5.8.16.77",
"FileHash": "E1B85D995DC09DE25603D0B7A67D998015F6C045",
"OldFileHash": "B276263D373A6B56EEAB09673429E1490AEFC5E14738CDF9E1661C36EBD80656",
"RequestUrl": "https://kaspersky.com/"
}
```

2 Saving the event in the CyberTrace database

If integration over TCP is used, CyberTrace uses regular expressions to extract indicators from the event. If integrated via the REST API (using API lookup), indicators are passed directly in the body of the request. If at the moment when an indicator is processed, the feeds do not contain information that allows to classify it, CyberTrace saves the indicator to the retroscan database for subsequent analysis after feeds are updated.

3 Running the retroscan task

The retroscan task can be scheduled or run manually. To run a retroscan manually, go to the **System** → **Retroscan** page and click **Start now**.

4 Detecting indicators after a feed update

If, during the update process, the feeds deliver indicators that match previously saved events, CyberTrace detects such matches when running the retroscan task.

5 Generating alerts based on retroscan results

After the retroscan is completed, CyberTrace generates alerts about the detection of indicators of compromise and sends these alerts to the KUMA collector.

Example alert

```
Category=KUMA_Demo_1_Hash_SHA1|MatchedIndicator=E1B85D995DC09DE25603D0B7A67D998015F6C045|MD5=5BA7335AD847E5ED6211FB27
05:34|geo=bd, eg, in|last_seen=02.02.2021 11:36|popularity=2|threat=HEUR:Trojan.MSIL.Taskun.gen
```

6 Event processing in KUMA

The event is processed by the **[OOTB] CyberTrace** normalizer. The user can match the received notification with the original event for subsequent analysis.

7 Getting a service alert about the completion of the task

If CyberTrace is configured to send service alerts, CyberTrace sends an alert about the completion of the retroscan task.

Example alert

```
Jun 05 16:08:33
alert=KL_ALERT_RetroScanCompleted|iocs_detected=168|iocs_rescanned=1511177|retroscan_report=https://127.0.0.1/retrosc
C2DF-4AED-B430-2E64AEF781FC
```

Integration with Kaspersky Threat Intelligence Portal

The Kaspersky Threat Intelligence Portal combines all of Kaspersky's knowledge about cyberthreats and how they're related into a single web service. When integrated with KUMA, the portal helps KUMA users to make faster and better-informed decisions, providing them with data about URLs, domains, IP addresses, including WHOIS and DNS data.

In the Kaspersky Threat Intelligence Portal Help, you can find information about data provision for the following objects:

- Hashes
- IP addresses
- Domains
- Web addresses

Access to the Kaspersky Threat Intelligence Portal is provided based on a fee. License certificates are created by Kaspersky staff. To obtain a certificate for Kaspersky Threat Intelligence Portal, contact your Kaspersky Technical Account Manager.

Initializing the Kaspersky Threat Intelligence Portal integration

To integrate Kaspersky Threat Intelligence Portal into KUMA:

1. In the KUMA web interface, open the **Resources** section.
2. Under **Resources**, select **Secrets**.

   The list of available secrets will be displayed.
3. Click the **Add** button to create a new secret. This resource is used to store credentials of your Kaspersky Threat Intelligence Portal account.

   The secret window is displayed.
4. Enter information about the secret:

   a. In the **Name** field, choose a name for the added secret.

   b. In the **Tenant** drop-down list, select the tenant that will own the created resource.

   c. In the **Type** drop-down list, select **ktl**.

   d. In the **User** and **Password** fields, enter credentials for your Kaspersky Threat Intelligence Portal account.
5. Upload your Kaspersky Threat Intelligence Portal certificate key:

   a. Click the **Upload PFX** button and select the PFX file with your certificate.

      The name of the selected file appears to the right of the **Upload PFX** button.

   b. Enter the password to the PFX file in the **PFX password** field.
6. If necessary, select one or more tags for the secret from the **Tags** drop-down list.
7. If you want, enter a **Description** of the secret.
8. Click **Create**.

   The Kaspersky Threat Intelligence Portal account credentials are now saved and can be used in other KUMA resources.
9. Go to the **Settings** → **Integrations** → **Kaspersky Threat Lookup integration**.
10. Use the **Status** toggle switch to enable the integration. The integration is disabled by default.
11. In the **Secret** drop-down list, select the secret you created before.

    You can create a new secret by clicking the button with the plus sign. The created secret will be saved in the **Resources** → **Secrets** section.
12. If necessary, select a proxy server in the **Proxy** drop-down list.

13. If you want to accept the License Agreement for OSINT data, click the **License Agreement** link. This opens the **License Agreement** window; in that window, select **I accept the License Agreement** and click **Save**. KUMA will start to receive OSINT data after you send a data enrichment request from Kaspersky Threat Intelligence Portal by selecting the **OSINT data** check box in the enrichment settings.

14. Click **Save**.

15. After you save the settings, log in to the web interface and accept the **Terms of Use**. Otherwise, an error will be returned in the API.

The integration process of Kaspersky Threat Intelligence Portal with KUMA is completed.

Once Kaspersky Threat Intelligence Portal and KUMA are integrated, you can request additional information from the event details area about hosts, domains, URLs, IP addresses, and file hashes (MD5, SHA1, SHA256).

Requesting information from Kaspersky Threat Intelligence Portal

To request information from Kaspersky Threat Intelligence Portal:

1. Open the event details area from the events table, alert window, or correlation event window and click the link on a domain, web address, IP address, or file hash.

   The **Threat Lookup enrichment** area opens in the right part of the screen.

2. Select check boxes next to the data types you want to request.

   If neither check box is selected, all information types are requested.

3. In the **Maximum number of records in each data group** field enter the number of entries per selected information type you want to receive. The default value is `10`.

4. Click **Request**.

A *kt1* task has been created. When it is completed, events are enriched with data from Kaspersky Threat Intelligence Portal which can be viewed from the events table, Alert window, or correlation event window.

Viewing information from Kaspersky Threat Intelligence Portal

To view information from Kaspersky Threat Intelligence Portal:

Open the event details area from the events table, alert window, or correlation event window and click the link on a domain, web address, IP address, or file hash for which you previously requested information from Kaspersky Threat Intelligence Portal.

The event details area opens in the right part of the screen with data from Kaspersky Threat Intelligence Portal; the time when it was received is indicated at the bottom of the screen.

Information received from Kaspersky Threat Intelligence Portal is cached. If you click a domain, web address, IP address, or file hash in the event details pane for an event for which KUMA has information available, instead of the **Threat Lookup enrichment** window, the data from Kaspersky Threat Intelligence Portal is displayed, with the time when it was received indicated. You can update the data.

Updating information from Kaspersky Threat Intelligence Portal

To update information, received from Kaspersky Threat Intelligence Portal:

1. Open the event details area from the events table, alert window, or correlation event window and click the link on a domain, web address, IP address, or file hash for which you previously requested information from Kaspersky Threat Intelligence Portal.

2. Click **Update** in the event details area containing the data received from the Kaspersky Threat Intelligence Portal.

   The **Threat Lookup enrichment** area opens in the right part of the screen.

3. Select the check boxes next to the types of information you want to request.

   If neither check box is selected, all information types are requested.

4. In the **Maximum number of records in each data group** field enter the number of entries per selected information type you want to receive. The default value is `10`.

5. Click **Update**.

   The *KTL* task is created and the new data received from Kaspersky Threat Intelligence Portal is requested.

6. Close the **Threat Lookup enrichment** window and the details area with KTL information.

7. Open the event details area from the events table, Alert window or correlation event window and click the link on a domain, URL, IP address, or file hash for which you updated Kaspersky Threat Intelligence Portal information and select **Show info from Threat Lookup**.

The event details area opens on the right with data from Kaspersky Threat Intelligence Portal, indicating the time when it was received on the bottom of the screen.

Integration with R-Vision Security Orchestration, Automation and Response

R-Vision Security Orchestration, Automation and Response (hereinafter referred to as R-Vision SOAR) is a software platform used for automation of monitoring, processing, and responding to information security incidents. It aggregates cyberthreat data from various sources into a single database for further analysis and investigation to facilitate incident response capabilities.

R-Vision SOAR can be integrated with KUMA. When this integration is enabled, the creation of a KUMA alert triggers the creation of an incident in R-Vision SOAR. A KUMA alert and its R-Vision SOAR incident are interdependent. When the status of an incident in R-Vision SOAR is updated, the status of the corresponding KUMA alert is also changed.

Integration of R-Vision SOAR and KUMA is configured in both solutions. In KUMA integration settings are available only for general administrators.

Mapping KUMA alert fields to R-Vision SOAR incident fields when transferring data via API

KUMA alert field	R-Vision SOAR incident field
`FirstSeen`	`detection`
`priority`	`level`
`correlationRuleName`	`description`
`events` As a JSON file	`files`

Configuring integration in KUMA

This section describes integration of KUMA with R-Vision SOAR from the KUMA side.

Integration in KUMA is configured in the web interface under **Settings** → **Integrations** → **IRP/SOAR**.

To configure integration with R-Vision SOAR:

1. Open the **Resources** section of the KUMA web interface and under **Resources**, select **Secrets**.

   The list of available secrets will be displayed.

2. Click the **Add** button to create a new secret. This resource is used to store token for R-Vision SOAR API requests.

   The secret window is displayed.

3. Enter information about the secret:

   a. In the **Name** field, enter a name for the added secret. The name must contain 1 to 128 Unicode characters.

   b. In the **Tenant** drop-down list, select the tenant that will own the created resource.

   c. In the **Type** drop-down list, select **token**.

   d. In the **Token** field, enter your R-Vision SOAR API token.

      You can obtain the token in the R-Vision SOAR web interface under **Settings** → **Common** → **API**.

   e. If necessary, select the tags for the secret from the **Tags** drop-down list.

   f. If necessary, in the **Description** field, add up to 4,000 Unicode characters describing the secret.

4. Click **Create**.

   The R-Vision SOAR API token is now saved and can be used in other KUMA resources.

5. In the KUMA web interface, go to the **Settings** → **Integrations** → **IRP / SOAR** section.

   The window containing R-Vision SOAR integration settings opens.

6. Use the **State** toggle switch to enable the integration of the R-Vision SOAR with KUMA. The integration is disabled by default.

7. In the **Secret** drop-down list, select the previously created secret.

   You can create a new secret by selecting **Create**. The created secret is saved in the **Resources** → **Resources** → **Secrets**.

8. In the **URL** specify the URL of the R-Vision SOAR server host.

9. In the **Field name where KUMA alert IDs must be placed**, specify the name of the R-Vision SOAR field where the ID of the KUMA alert must be written.

10. In the **Field name where KUMA alert URLs must be placed** field, specify the name of the R-Vision SOAR field where the link to the KUMA alert must be written.

11. In the **Category** field, specify the category of the R-Vision SOAR incident that is created after alert information is received from KUMA.

12. In the **KUMA event fields that must be sent to IRP / SOAR** drop-down list, select the KUMA event fields to be sent to R-Vision SOAR.

13. Under **Severity**, specify the thresholds for mapping KUMA severity levels to R-Vision SOAR severity levels.

14. Click **Save**.

In KUMA integration with R-Vision SOAR is now configured. If integration is also configured in R-Vision SOAR, when alerts appear in KUMA, information about those alerts will be sent to R-Vision SOAR to create an incident. The **Details on alert** section in the KUMA web interface displays a link to R-Vision SOAR.

If you are working with multiple tenants and want to integrate with R-Vision SOAR, the names of tenants must match the abbreviated names of companies in R-Vision SOAR.

Adding the ALERT_ID and ALERT_URL incident fields

To add the ALERT_ID incident field in the R-Vision SOAR:

1. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Incident fields**, select the **No group** group of fields.

2. Click the plus icon in the right part of the screen.

   The right part of the screen will display the settings area for the incident field you are creating.

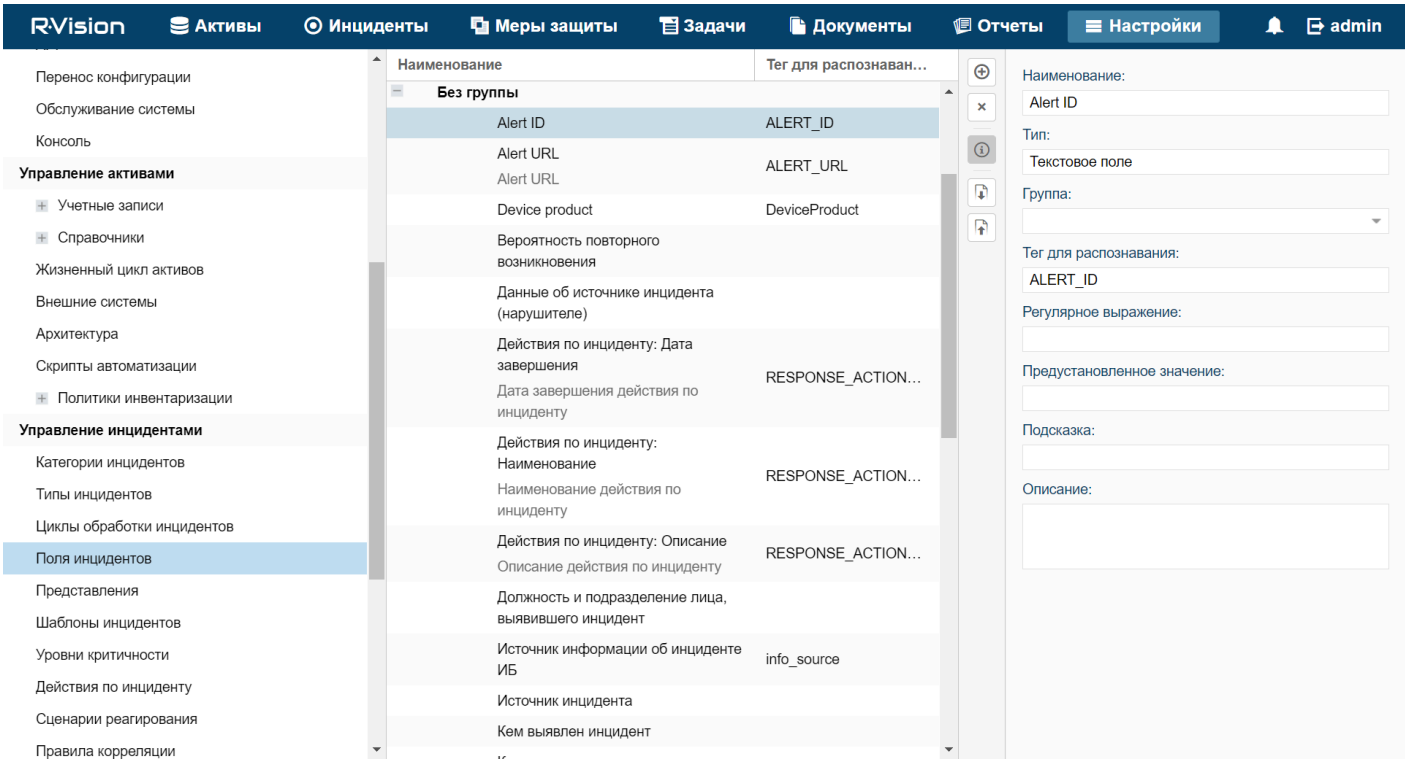
3. In the **Title** field, enter the name of the field (for example: `Alert ID`).

4. In the **Type** drop-down list, select **Text field**.

5. In the **Parsing Tag** field, enter `ALERT_ID`.

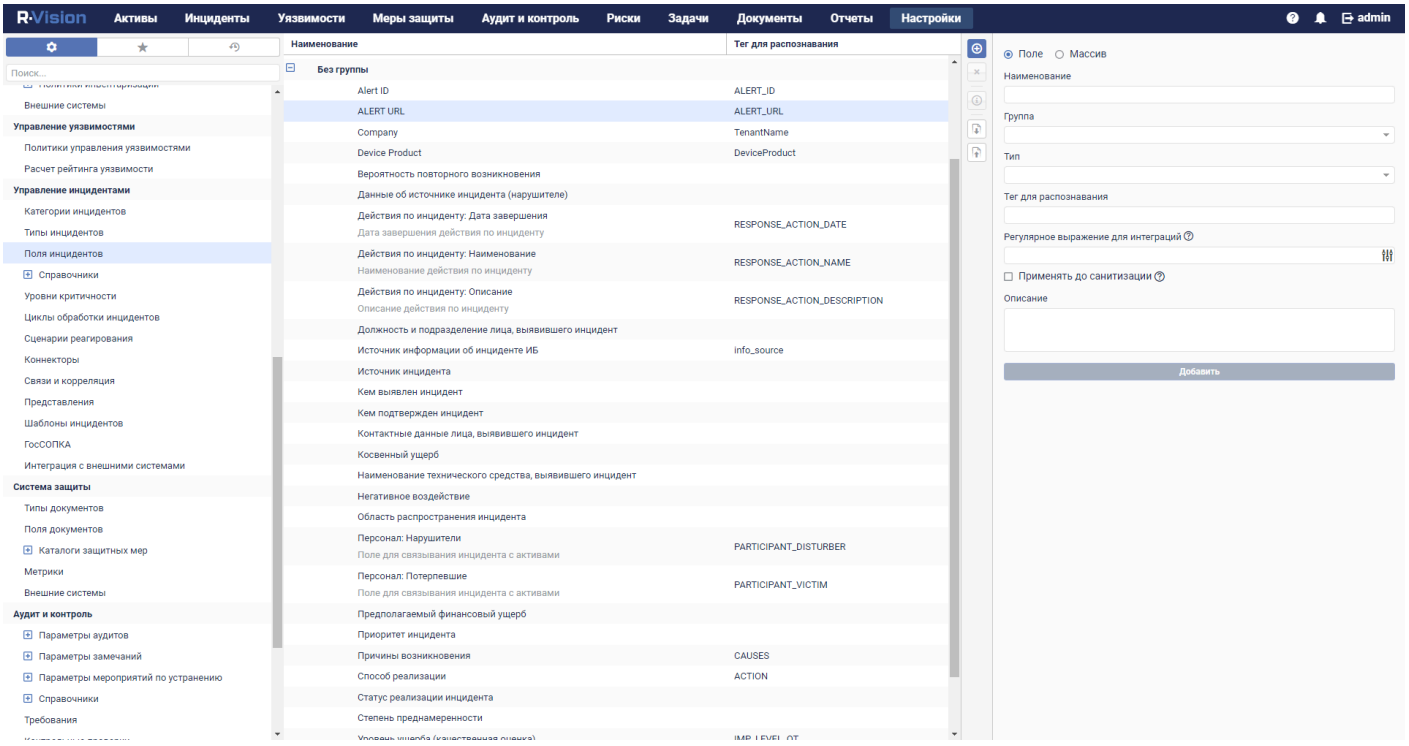
The `ALERT_ID` field will be added to the R-Vision SOAR incident (click the links below to see images).

ALERT_ID field in R-Vision SOAR version 4.0



Adding the ALERT_ID field in R-Vision SOAR 4.0

ALERT_ID field in R-Vision SOAR version 5.0



Adding the ALERT_ID field in R-Vision SOAR 5.0

To add the ALERT_URL incident field in R-Vision SOAR:

1. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Incident fields**, select the **No group** group of fields.

2. Click the plus icon in the right part of the screen.

   The right part of the screen will display the settings area for the incident field you are creating.

3. In the **Title** field, enter the name of the field (for example: `Alert URL`).

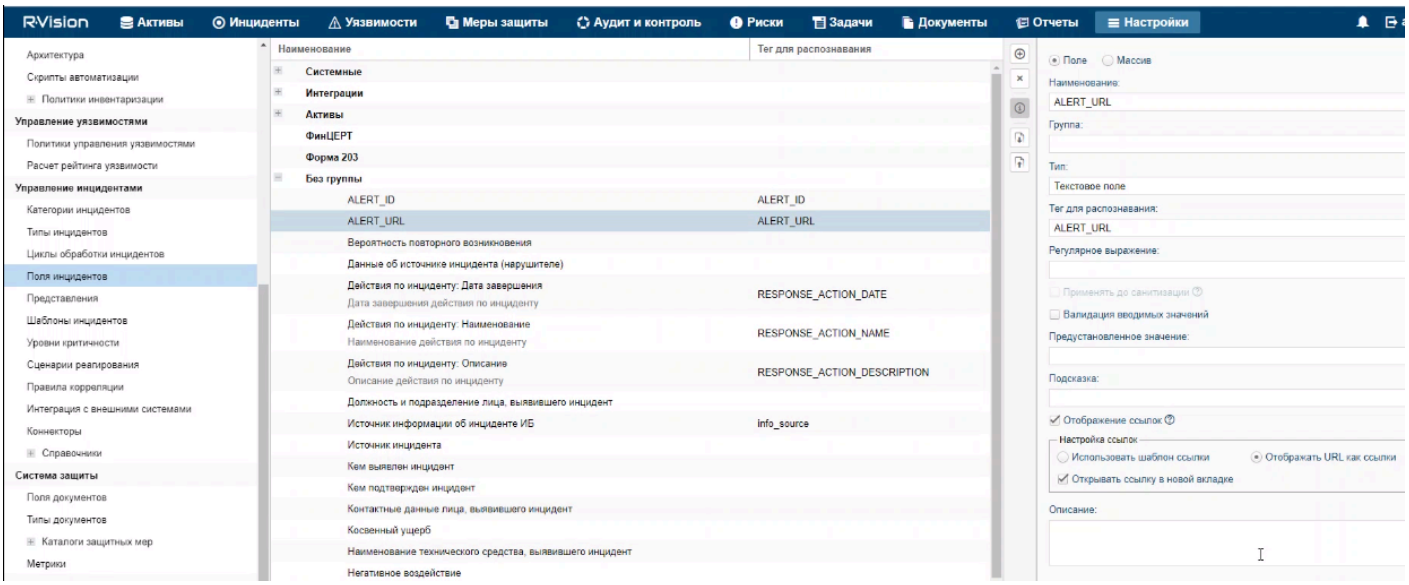
4. In the **Type** drop-down list, select **Text field**.

5. In the **Parsing Tag** field, enter `ALERT_URL`.

6. Select the **Display links** and **Display URL as links** check boxes.

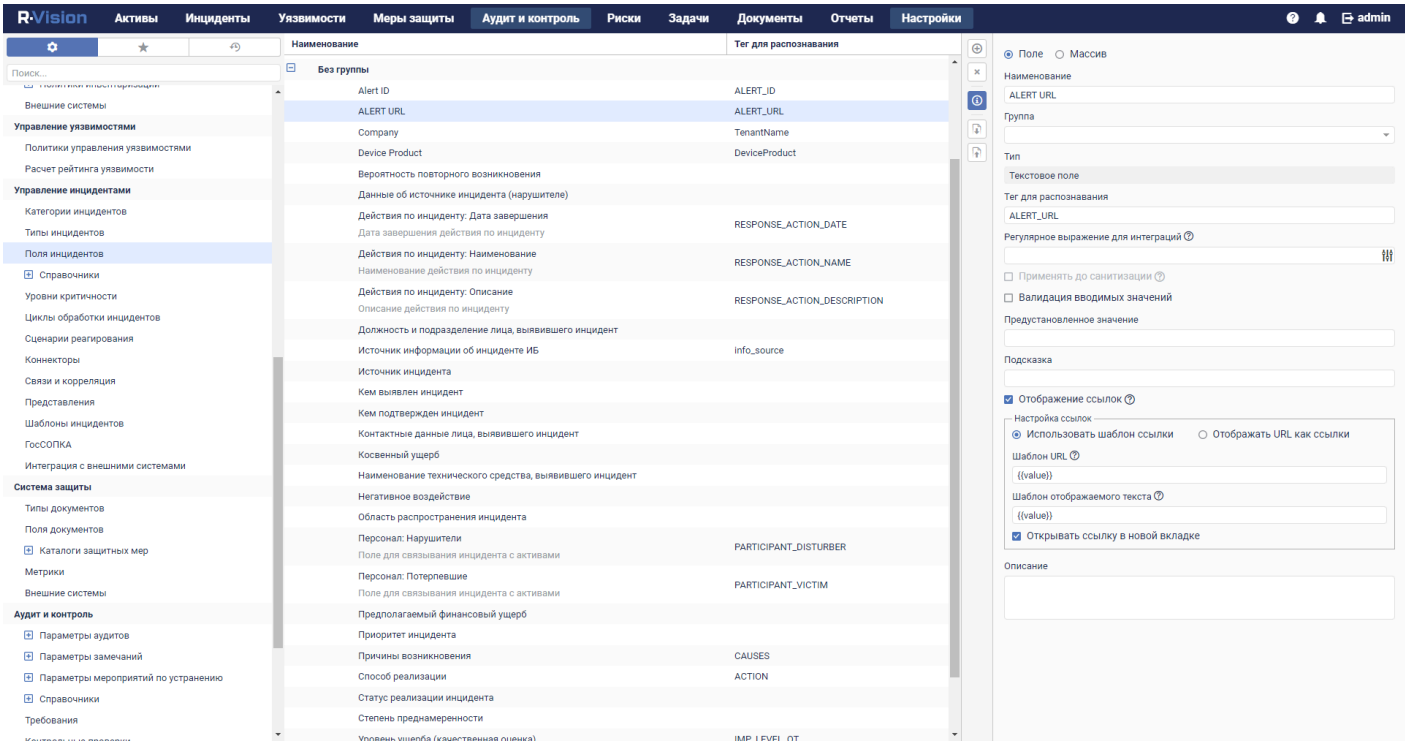
The `ALERT_URL` field will be added to the R-Vision SOAR incident (click the links below to see images).

ALERT_URL field in R-Vision SOAR version 4.0



Adding the ALERT_URL field in R-Vision SOAR 4.0

ALERT_URL field in R-Vision SOAR version 5.0



Adding the ALERT_URL field in R-Vision SOAR 5.0

If necessary, you can likewise configure the display of other data from a KUMA alert in an R-Vision SOAR incident.

Creating a collector in R-Vision SOAR

To create a collector in R-Vision SOAR:

1. In the R-Vision SOAR web interface, under **Settings** → **Common** → **Collectors**, click the plus icon.
2. Specify the collector name in the **Name** field (for example, `Main collector`).
3. In the **Collector address** field, enter the IP address or hostname where the R-Vision SOAR is installed (for example, `127.0.0.1`).
4. In the **Port** field type `3001`.
5. Click **Add**.
6. On the **Organizations** tab, select the organization for which you want to add integration with KUMA and select the **Default collector** and **Response collector** check boxes.

The R-Vision SOAR collector is created.

Creating connector in R-Vision SOAR

To create connector in R-Vision SOAR:

1. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Connectors**, click the plus icon.
2. In the **Type** drop-down list, select **REST**.
3. In the **Name** field, specify the connector name, such as `KUMA`.
4. In the **URL** field, enter an API request to close an alert in the following format: `<FQDN of the KUMA Core server>:<port used for API requests (7223 by default)>/api/v1/alerts/close`.

   Example
   ```
   https://kuma.example.com:7223/api/v1/alerts/close
   ```

5. In the **Authorization type** drop-down list, select **Token**.
6. In the **Auth header** field enter the following:

   ```
   Authorization
   ```

7. In the **Auth value** field enter the token of KUMA user with general administrator role in the following format:

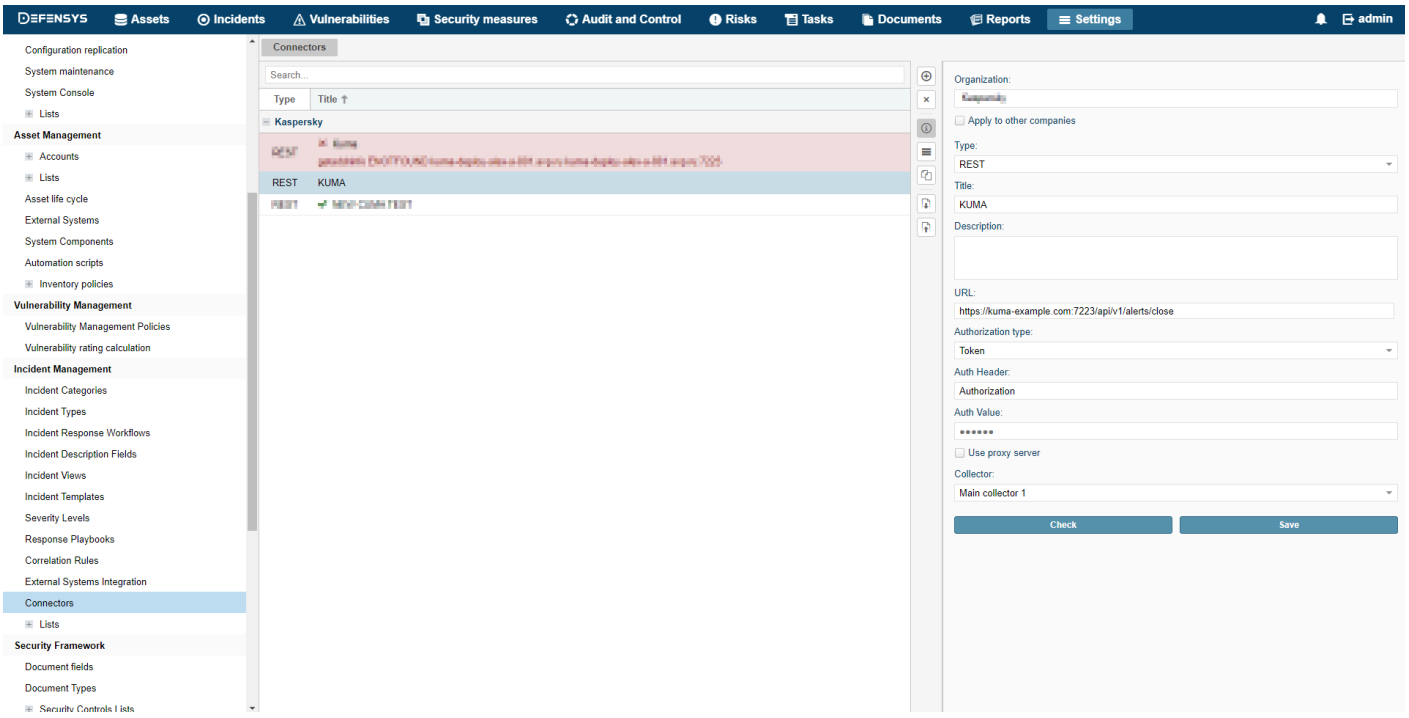
   ```
   Bearer <KUMA General administrator token>
   ```

8. In the **Collector** drop-down list select previously created collector.

9. Click **Save**.

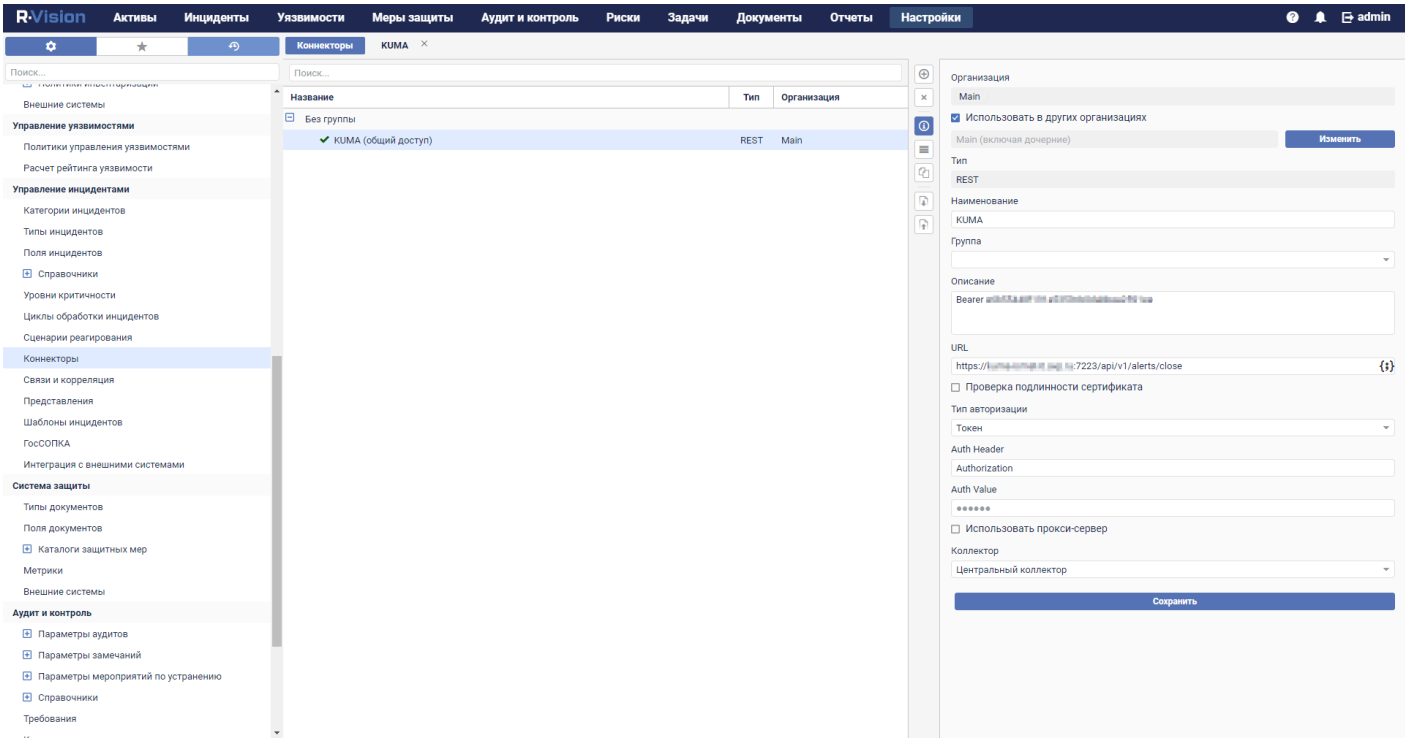
The connector is created (click the links below for images).

Connector in R-Vision SOAR version 4.0



Connector in R-Vision SOAR version 4.0

Connector in R-Vision SOAR version 5.0



Connector in R-Vision SOAR version 5.0

When connector is created you must configure sending API queries for closing alerts in KUMA.

To configure API queries in R-Vision SOAR:

1. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Connectors**, open for editing the newly created connector.

2. In the request type drop-down list, select **POST**.

3. In the **Params** field, enter the API request to close an alert in the following format: `<FQDN of the KUMA Core server>:<port used for API requests (7223 by default)>/api/v1/alerts/close`.

   Example

   ```
   https://kuma.example.com=10214746:7223/api/v1/alerts/close
   ```

   On the **HEADERS** tab, add the following keys and values:

   - Key:

     ```
     Content-Type
     ```

     Value:

     ```
     application/json
     ```

   - Key:

     ```
     Authorization
     ```

     Value:

     ```
     Bearer <KUMA General administrator token>
     ```

     The token of the KUMA general administrator can be obtained in the KUMA web interface under **Settings** → **Users**.

4. On the **BODY** → **Raw** tab, enter the body of the API request:

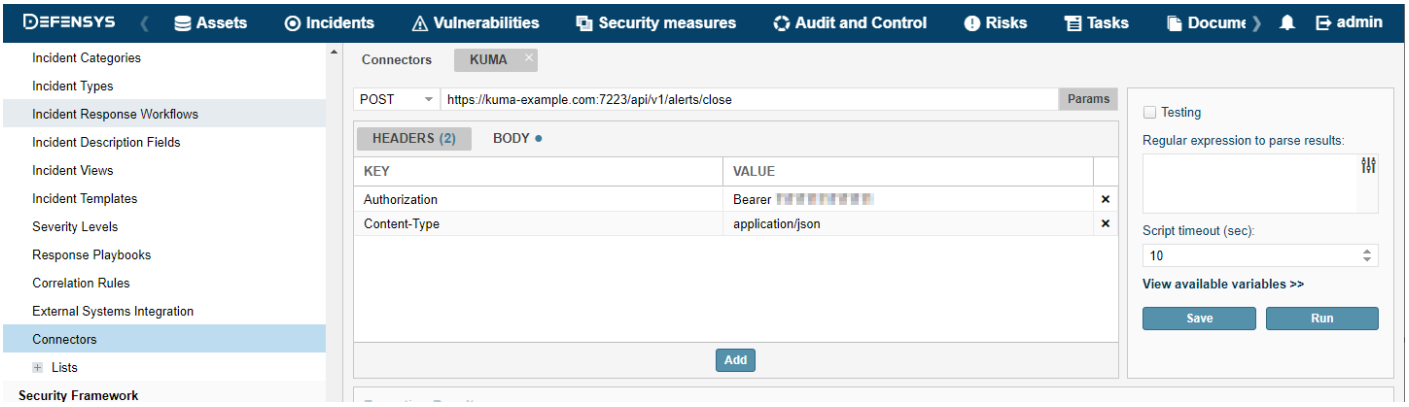
   ```
   {
       "id":"{{tag.ALERT_ID}}",
   "reason":"<Reason for closing the alert.Available values: "Incorrect Correlation Rule", "Incorrect Data",
   "Responded".>"
   }
   ```

   For details on the reasons for closing the alert, see the description of the alert data model.

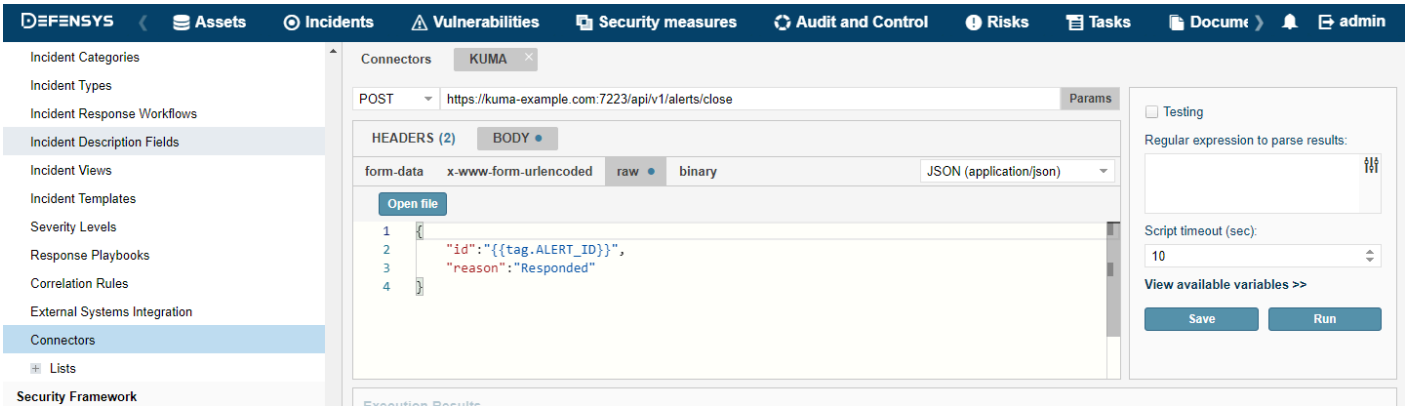
5. Click **Save**.

The connector is configured (click the links below for images).

Connector in R-Vision SOAR version 4.0

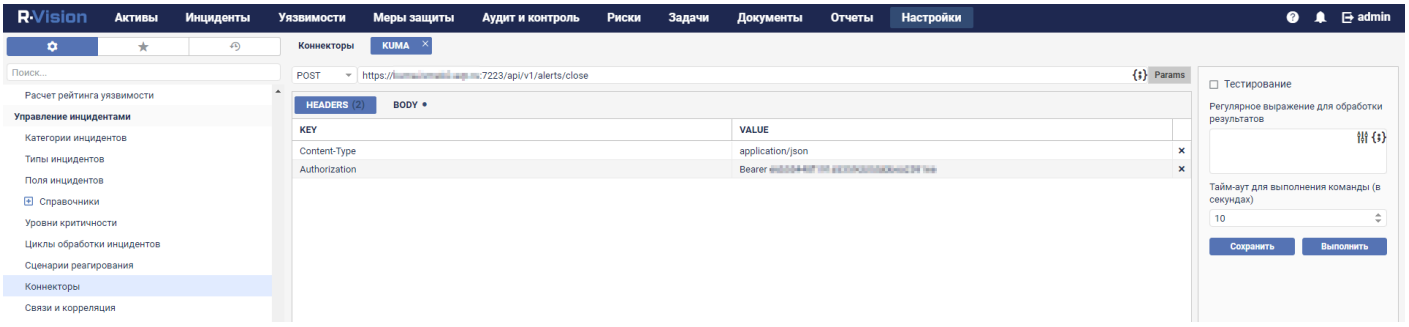


API request header

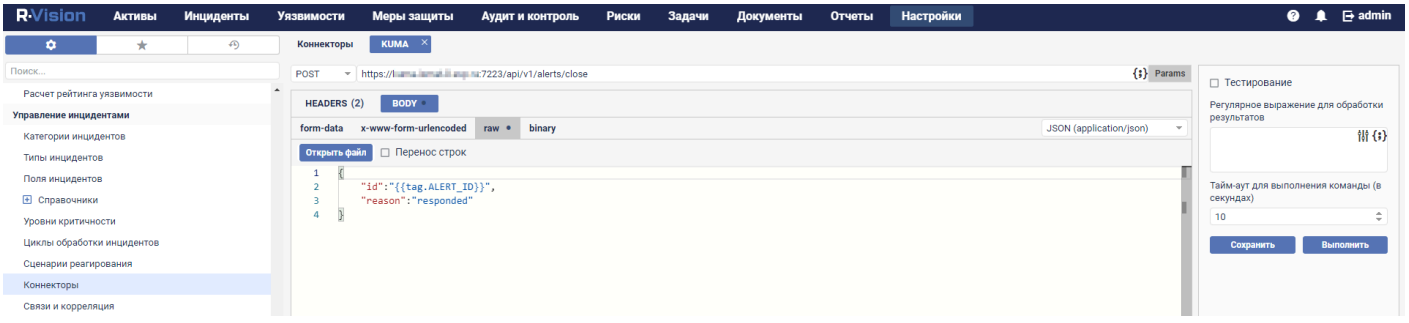


API request body

Connector in R-Vision SOAR version 5.0



API request header



API request body

Creating rule for closing KUMA alert when R-Vision SOAR incident is closed

To create a rule for sending an alert closing request to KUMA when an R-Vision SOAR incident is closed:

1. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Response playbooks**, click the plus icon.

2. In the **Name** field, type the name of the rule, for example, `Close alert`.

3. In the **Group** drop-down list select **All playbooks**.

4. Under **Autostart criteria**, click **Add** and enter the conditions for triggering the rule in the opened window:

   a. In the **Type** drop-down list, select **Field value**.

   b. In the **Field** drop-down list, select **Incident status**.

   c. Select the **Closed** status.

   d. Click **Add**.

   Rule trigger conditions are added. The rule will trigger when an incident is closed.

5. Under **Incident Response Actions**, click **Add** → **Run connector**. In the window that is opened, select the connector that you want to be run when the rule is triggered:

   a. In the **Connector** drop-down list select previously created connector.

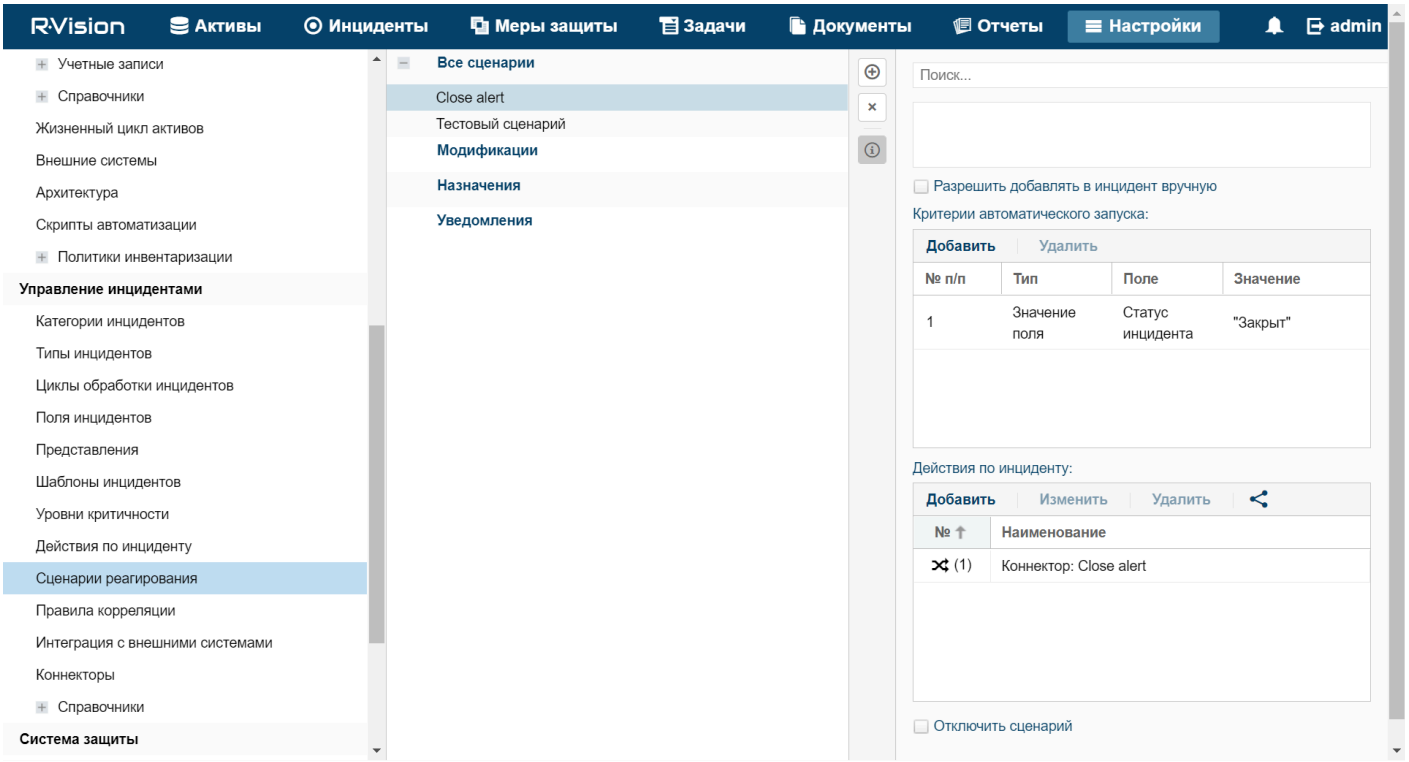
   b. Click **Add**.

   Connector added to the rule.

6. Click **Add**.

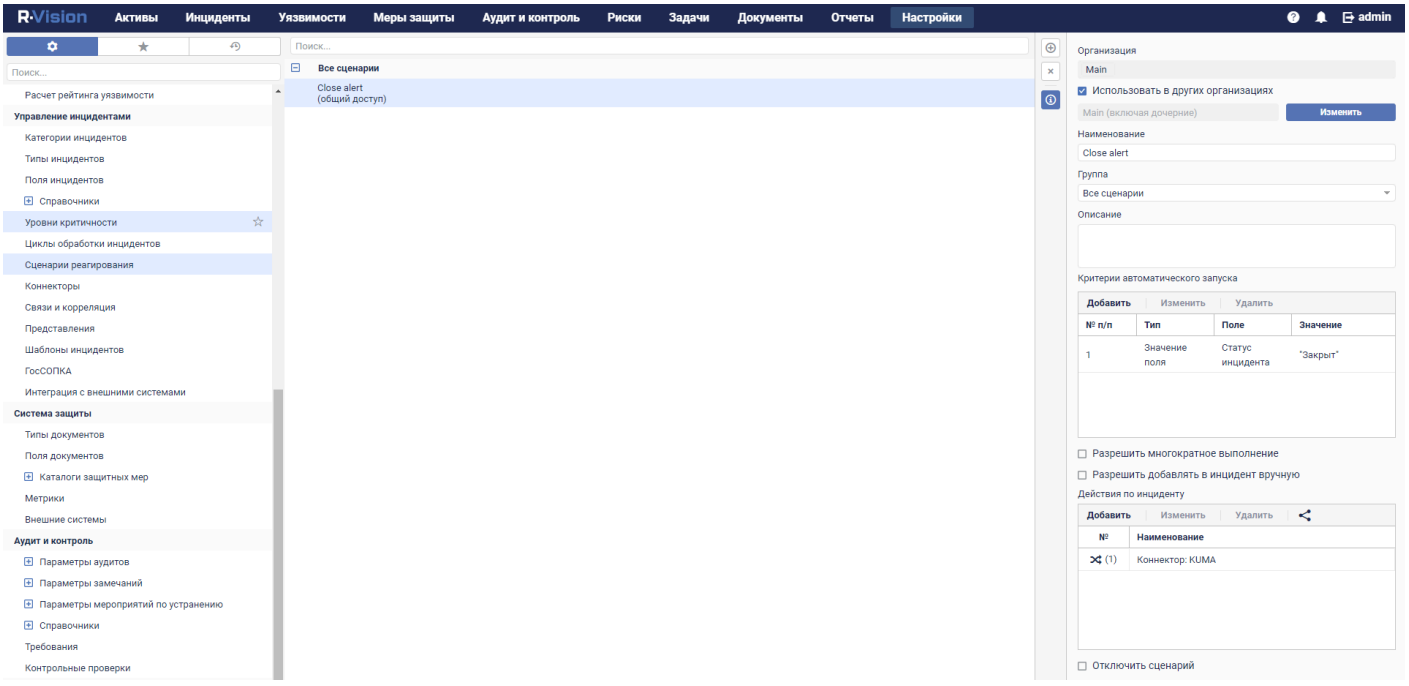
A rule is created for sending a KUMA alert closing request when an R-Vision SOAR incident is closed (click the links below to see images).

R-Vision IRP version 4.0 playbook rule



R-Vision SOAR version 4.0 playbook rule

R-Vision SOAR version 5.0 playbook rule



R-Vision IRP version 5.0 playbook rule

Configuring integration in R-Vision SOAR

This section describes KUMA integration with R-Vision SOAR from the R-Vision SOAR side.

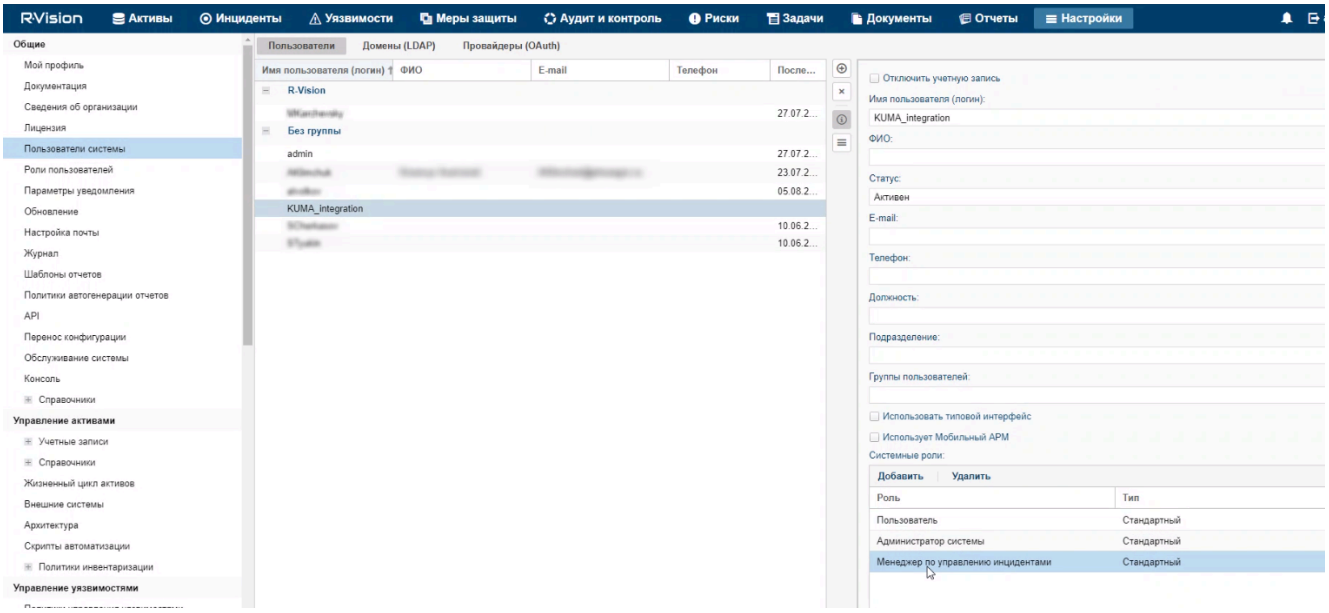
Integration in R-Vision SOAR is configured in the **Settings** section of the R-Vision SOAR web interface. For details on configuring R-Vision SOAR, please refer to the documentation on this application.

Configuring integration with KUMA consists of the following steps:

- **Configuring R-Vision SOAR user role**

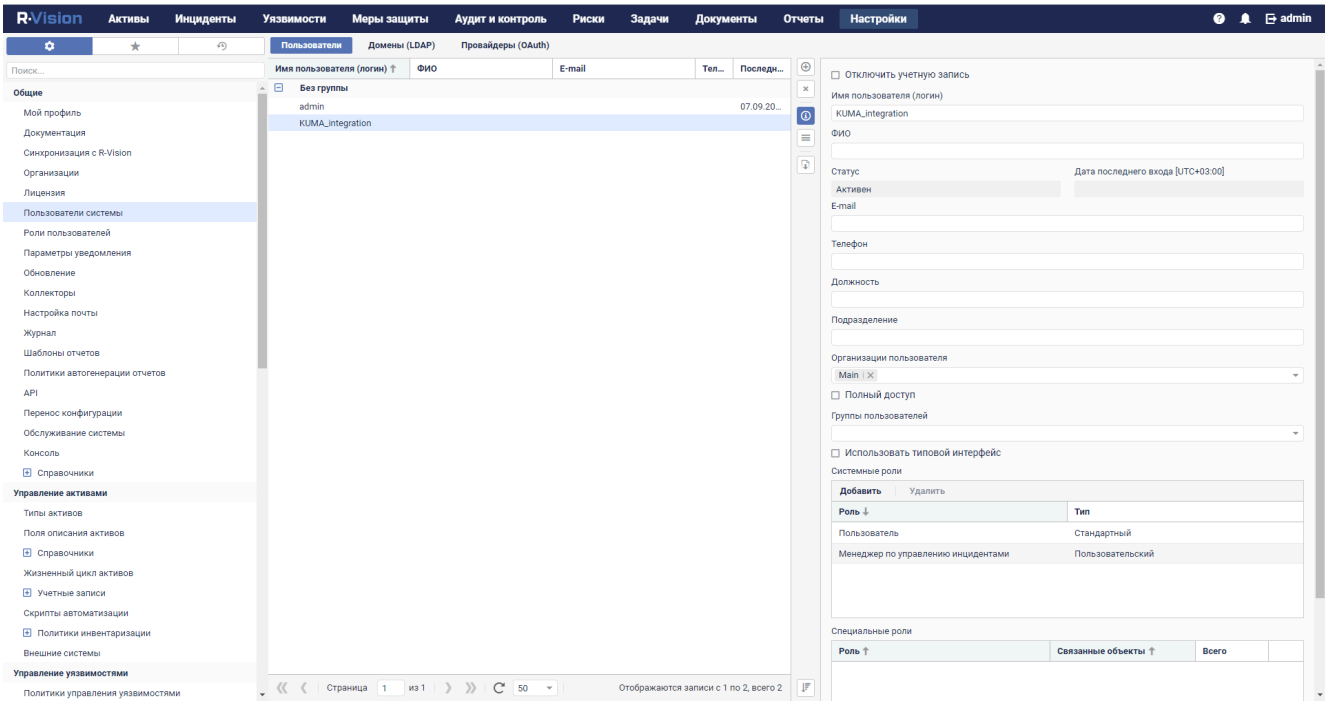
  1. Assign the **Incident manager** system role to the R-Vision SOAR user utilized for integration. The role is assigned when a user is selected in the R-Vision SOAR web interface in the **Settings** → **Common** → **System users** section. The role is added under **System roles** (click the links below for images).

     R-Vision SOAR version 4.0 user with the Incident Manager role



Assigning a role to a user in R-Vision SOAR 4.0

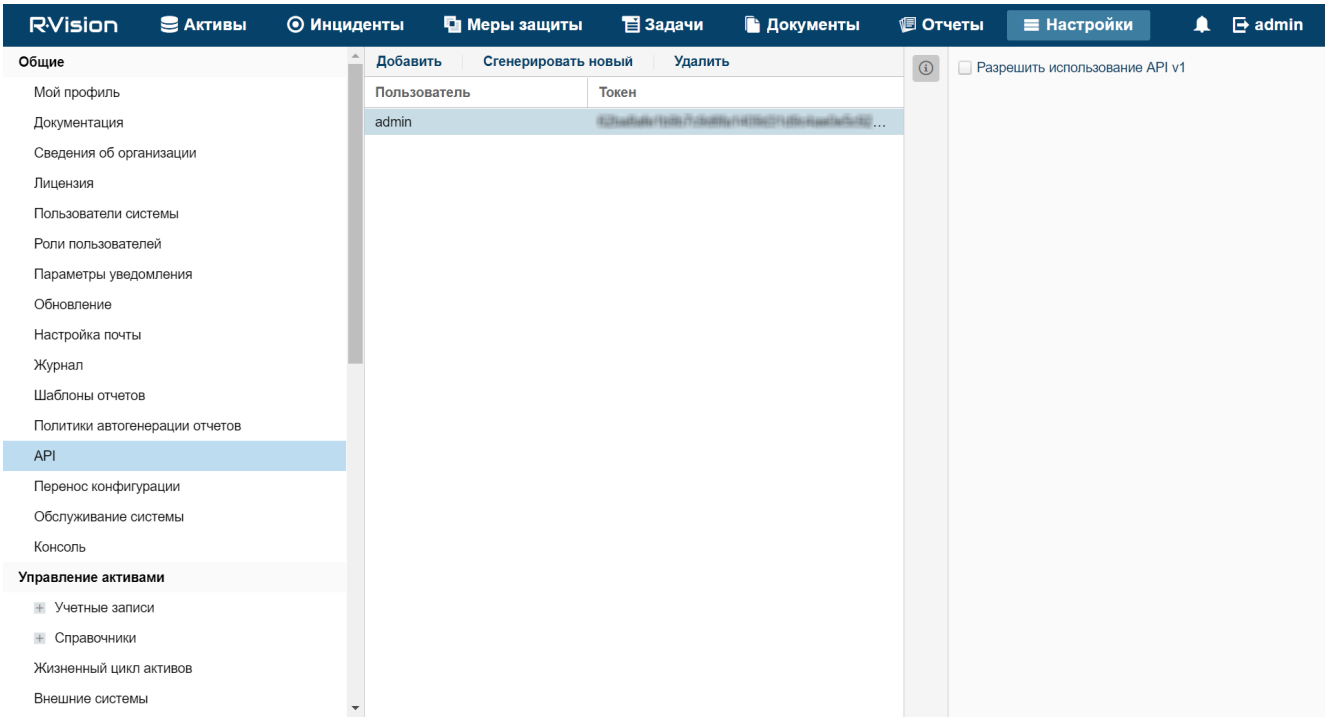
     R-Vision SOAR version 5.0 user with the Incident Manager role



Assigning a role to a user in R-Vision SOAR 5.0

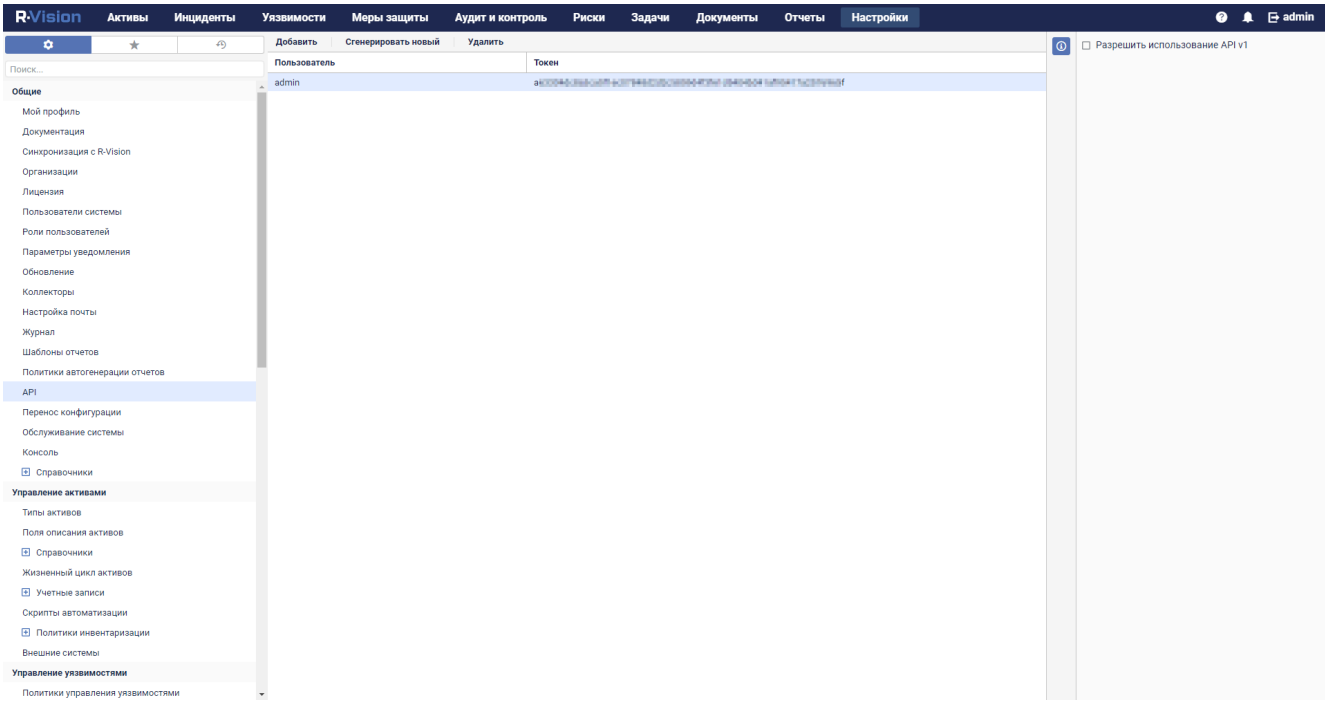
  2. Make sure that the API token of the R-Vision SOAR user utilized for integration is indicated [in the secret in the KUMA web interface](). The token is displayed in the R-Vision SOAR web interface under **Settings** → **Common** → **API** (click the links below for images).

API token in R-Vision SOAR version 4.0



API token in R-Vision SOAR version 4.0

API token in R-Vision SOAR version 5.0



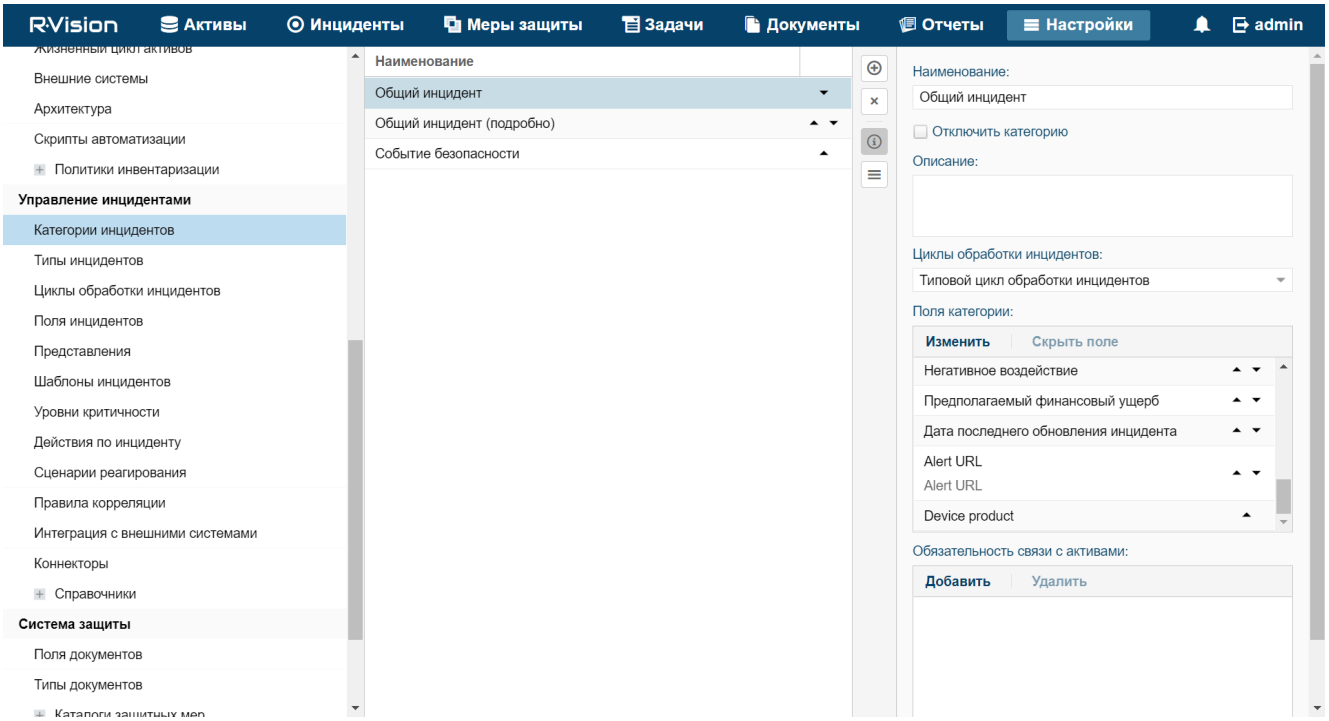
API token in R-Vision SOAR version 5.0

- **Configuring R-Vision SOAR incident fields and KUMA alert fields**

  1. Add the ALERT_ID and ALERT_URL incident fields.

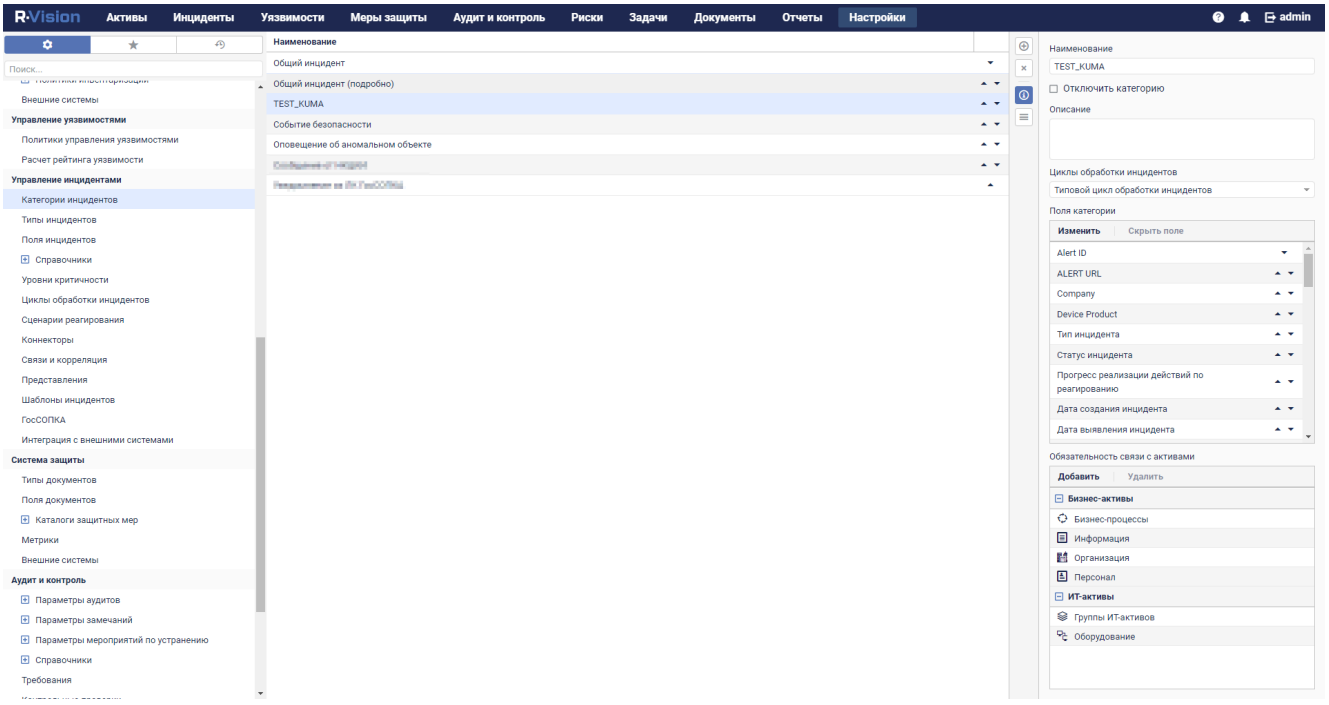
  2. Configure the category of R-Vision SOAR incidents created based on KUMA alerts. You can do this in the R-Vision SOAR web interface, in the **Settings** → **Incident management** → **Incident categories** section. Add a new incident category or edit an existing incident category by indicating the previously created `Alert ID` and `Alert URL` incident fields under **Category fields** (click the links below for images). The `Alert ID` field can be hidden.

Incident categories with data from KUMA alerts in R-Vision SOAR version 4.0



Configuring fields in incidents in R-Vision SOAR 4.0

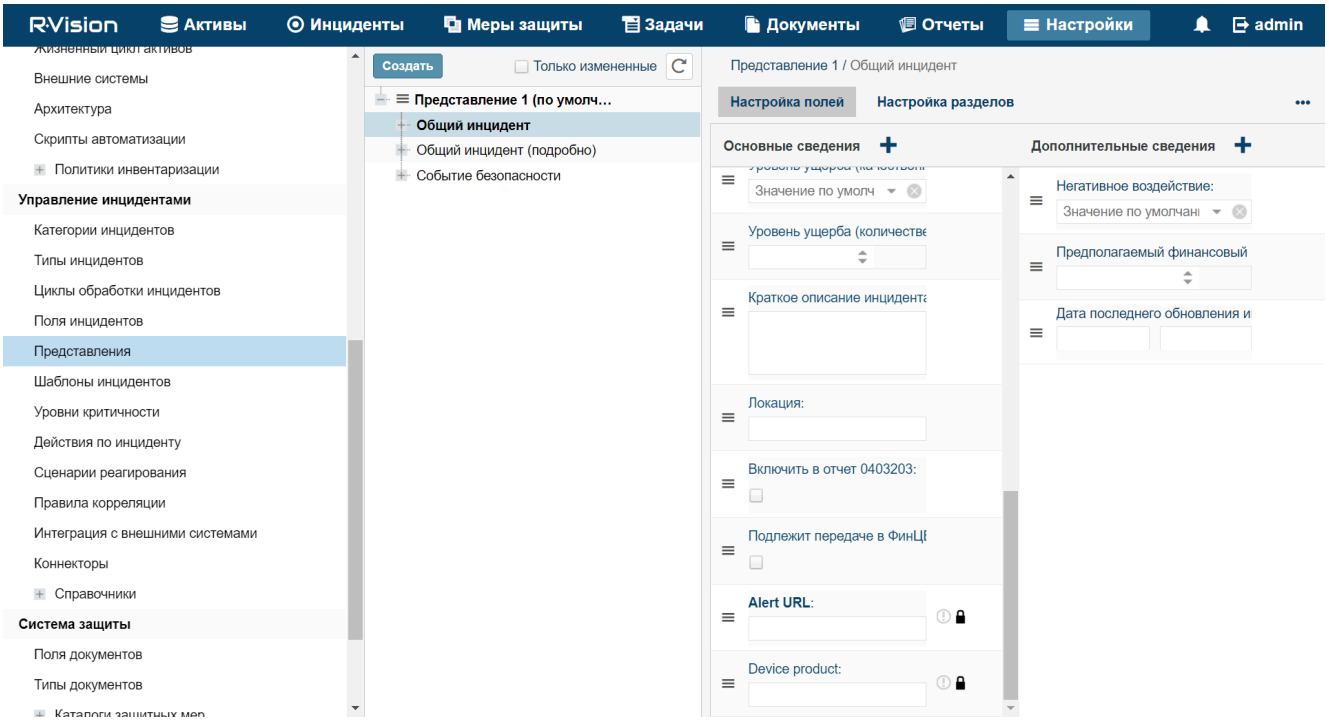
Incident categories with data from KUMA alerts in R-Vision SOAR version 5.0



Configuring fields in incidents in R-Vision SOAR 5.0

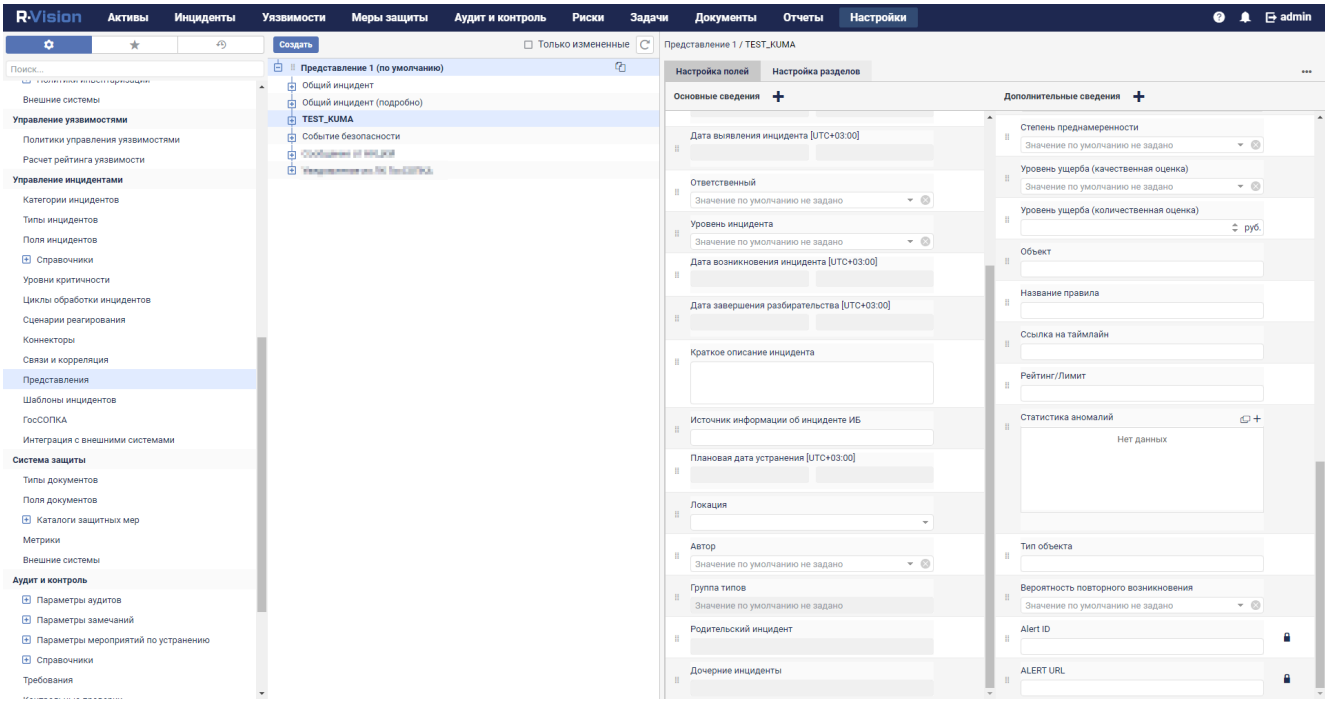
3. Block editing of previously created `Alert ID` and `Alert URL` incident fields. In the R-Vision SOAR web interface, under **Settings** → **Incident management** → **Presentation**, select the category of R-Vision SOAR incidents that will be created based on KUMA alerts and put a lock icon next to the `Alert ID` and `Alert URL` incident fields (click the links below for images).

The Alert URL field is not editable in R-Vision SOAR version 4.0



Preventing the editing of fields in R-Vision SOAR 4.0

The Alert URL field is not editable in R-Vision SOAR version 5.0



Preventing the editing of fields in R-Vision SOAR 5.0

- **Creating R-Vision SOAR collector and connector**

  1. Create an R-Vision SOAR collector to interact with KUMA.
  2. Create and configure an R-Vision SOAR connector to send API requests to close KUMA alerts.

- **Creating a rule to close a KUMA alert**

  Create a rule for sending KUMA alert closing request when R-Vision SOAR incident is closed.

Integration with KUMA is now configured in R-Vision SOAR. If integration is also configured in KUMA, when alerts appear in KUMA, information about those alerts is sent to R-Vision SOAR to create an incident. The **Details on alert** section in the KUMA web interface displays a link to R-Vision SOAR.

Managing alerts using R-Vision SOAR

After integration of KUMA and R-Vision SOAR is configured, data on KUMA alerts starts coming into R-Vision SOAR. Changes of alert parameters in KUMA are reflected in R-Vision SOAR. Any changes in the statuses of alerts in KUMA or R-Vision SOAR (except closing an alert) are also reflected in the other system.

Alert management scenarios when KUMA and R-Vision SOAR are integrated:

- **Send cyberthreat data from KUMA to R-Vision SOAR**

  Data on detected alerts is automatically sent from KUMA to R-Vision SOAR. An incident is also created in R-Vision SOAR.

  The following information about the KUMA alert is sent to R-Vision SOAR:

  - ID.
  - Name.
  - Status.
  - Date of the first event related to the alert.
  - Date of the last detection related to the alert.
  - User account name or email address of the security officer assigned to process the alert.
  - Alert severity.
  - Category of the R-Vision SOAR incident corresponding to the KUMA alert.
  - Hierarchical list of events related to the alert.
  - List of alert-related assets (internal and external).
  - List of users related to the alert.
  - Alert change log.
  - Link to the alert in KUMA.

- **Investigate cyberthreats in KUMA**

  Initial processing of an alert is performed in KUMA. The security officer can update and change any parameters of an alert except its ID and name. Any changes are reflected in the R-Vision SOAR incident card.

  If a cyberthreat turns out to be a false positive and its alert is closed in KUMA, its corresponding incident in R-Vision SOAR is also automatically closed.

- **Close incident in R-Vision SOAR**

  After all necessary work is completed on an incident and the course of the investigation is recorded in R-Vision SOAR, the incident is closed. The corresponding KUMA alert is also automatically closed.

- **Open a previously closed incident**

  If active monitoring detects that an incident was not completely resolved or if additional information comes up, this incident is re-opened in R-Vision SOAR. However, the alert remains closed in KUMA.

  The security officer can use a link to navigate from an R-Vision SOAR incident to the corresponding alert in KUMA and make the necessary changes to any of its parameters except the ID, name, and status of the alert. Any changes are reflected in the R-Vision SOAR incident card.

  Further analysis is performed in R-Vision SOAR. When the investigation is complete and the incident is closed again in R-Vision SOAR, the status of the corresponding alert in KUMA remains closed.

- **Request additional data from the source system as part of the response playbook or manually**

  If additional information is required from KUMA when analyzing incidents in R-Vision SOAR, in R-Vision SOAR, you can create a search request to KUMA (for example, you can request telemetry data, reputation, host information). This request is sent via KUMA REST API and the response is recorded in the R-Vision SOAR incident card for further analysis and reporting.

  This same sequence of actions is performed during automatic processing if it is not possible to immediately save all information on an incident during an import.

Integration with Active Directory, Active Directory Federation Services and FreeIPA

You can integrate KUMA with the Active Directory®, Active Directory Federation Services, and FreeIPA services used in your organization.

You can configure a connection to the Active Directory catalog service over the LDAP protocol. This lets you use information from Active Directory in correlation rules for enrichment of events and alerts, and for analytics.

If you configure a connection to a domain controller server, you can use domain authorization. In this case, you can bind the domain groups of users to the KUMA role filters. The users belonging to these groups will be able to use their domain account credentials to log in to the KUMA web interface and will obtain access to solution sections based on their assigned role.

> It is recommended to create the groups of users in Actions Active Directory, Active Directory Federation Services, or FreeIPA in advance if you want to provide such groups with the capability for authorization using their domain account in the KUMA web interface. An email address must be indicated in the properties of a user account in Active Directory.

Establishing a LDAP connection to Active Directory

LDAP connections are created and managed in the **Settings** → **Integrations** → **LDAP server** section of the KUMA web interface. The **LDAP server** section displays the tenants for which LDAP connections have been created. Tenants can be added or removed.

When you select a help tenant, the **LDAP Server Integration** pane opens, which displays a table with existing LDAP connections. Connections can be created or modified. In this window, you can change the frequency of queries sent to LDAP servers and set the retention period for obsolete data.

After enabling the integration, information about Active Directory accounts becomes available in the details of alerts, correlation events, and incidents. If you click an account name in the **Related users** section of the window, the **Account details** window opens with the data imported from Active Directory.

Data from Active Directory can also be used when enriching events in collectors and in analytics.

Imported Active Directory attributes

The following account attributes can be requested from Active Directory:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `company`
- `department`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `ipaUniqueID`
- `l`
- `mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (this attribute can be used for search during correlation)
- `mobile`
- `objectGUID` (this attribute always requested from Active Directory even if a user doesn't specify it)
- `objectSid`
- `physicalDeliveryOfficeName`
- `sAMAccountName`
- `sAMAccountType`

- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `userPrincipalName`
- `whenChanged`
- `whenCreated`

For details about Active Directory attributes, please refer to the Microsoft documentation.

Enabling and disabling LDAP integration

You can enable or disable all LDAP connections of the tenant at the same time, or enable and disable an LDAP connection individually.

To enable or disable all LDAP connections of a tenant:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section and select the tenant for which you want to enable or disable all LDAP connections.
2. Do one of the following:
   a. Set the toggle switch in the **Status** column to **Enabled** or **Disabled**.
   b. Click the name of the tenant in the **Tenant** column to open the **LDAP server integration** sidebar, and in this sidebar:
      - Set the **Status** toggle switch to **Enabled** or **Disabled**.
      - Click **Save**.

To enable or disable a specific LDAP connection:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section and select the tenant for which you want to enable or disable all LDAP connections.
2. Click the name of the tenant in the **Tenant** column to open the **LDAP server integration** sidebar, and in this sidebar, go to the **Connections** section.
3. Use the toggle switch in the **Status** column to enable or disable a specific LDAP connection.
4. Click **Save**.

Adding a tenant to the LDAP server integration list

To add a tenant to the list of tenants for integration with an LDAP server:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.

   The **LDAP server integration by tenant** window is displayed.

2. Click the **Add settings for a new tenant** button.

   The **LDAP server integration** panel will open on the right.

3. In the **Tenant** drop-down list, select the tenant that you need to add.

4. Click **Add**.

The selected tenant will be added to the LDAP server integration tenant list.

To remove a tenant from the list of tenants for integration with an LDAP server:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.

   The **LDAP server integration by tenant** window is displayed.

2. Select the check box next to the tenant that you want to remove, and click **Remove**.

3. Confirm removal of the tenant.

The selected tenant will be removed from the LDAP server integration tenant list.

Creating an LDAP server connection

To create a new LDAP connection to Active Directory:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.

2. Select or add a tenant for which you want to create an LDAP connection.

3. In the **LDAP server integration by tenant** pane, select a tenant from the list or add a new tenant by clicking **Add settings for a new tenant** for which you want to create an LDAP connection.

4. Under **Connections**, click the **Create** button.

   This opens the **Create connections** panel.

5. To use this LDAP connection, turn on the connection using the **State** toggle switch.

6. Specify a unique name for the LDAP connection. The length of the string must be 1 to 128 Unicode characters.

7. In the drop-down list, select a secret containing the credentials for connecting to the Active Directory server. To do so, follow one of these steps:

   - If you previously created a secret, in the **Secret** drop-down list, select the existing secret of the **credentials** type.

   - If you want to create a secret, click **Create**.

     This opens the **Create secret** panel.

     1. In the **Name** field, enter the name of the secret. It must contain 1 to 128 Unicode characters.

     2. In the **User** and **Password** fields, enter the credentials for connecting to the Active Directory server.

        You can enter the user name in one of the following formats: `<user name>@<domain>` or `<domain> <user name>`.

     3. If necessary, select the tags for the secret from the **Tags** drop-down list.

     4. If necessary, in the **Description** field, enter up to 4,000 Unicode characters describing the secret.

     5. Then click the **Create** button.

8. In the **URL** field, enter the address of the domain controller in the `<hostname or IP address of server>:<port>` format.

   If necessary, click the **Add** button to specify the addresses of several domain controller servers that may be needed if one of the servers is unavailable. All of the specified servers must reside in the same domain. Only one domain controller server can be specified in one field. If the first domain controller is unavailable, the system tries to connect to the next domain controller in the list, then the next again, until a connection can be established.

   If the host of the domain controller is not found when attempting to connect, for example, if a non-existent address is entered in the **URL** field, there is no switchover to the next domain controller address. KUMA returns an error instead.

9. Select one of the following TLS encryption types for connecting to the domain controller:

   - **LDAPS**.

     When using LDAPS, an encrypted connection is immediately established over port 636. This type of TLS encryption is configured by default.

   - **startTLS**.

     When the startTLS method is used, first it establishes an unencrypted connection to port 389, and then sends an encryption request. If the STARTTLS command ends with an error, the connection is terminated.

     > Make sure that port 389 is open. Otherwise, a connection with the domain controller will be impossible.

   - **Insecure**.

   When using an encrypted connection, it is impossible to specify an IP address as a URL.

10. In the **Certificate** drop-down list, specify an existing TLS-certificate of an accredited certification authority that was used to sign the LDAP server's certificate. Custom certificates cannot be used.

To do so, follow one of these steps:

- If you already have a certificate, select it from the drop-down list.
- If you want to create a certificate, click **Create**.

  This opens the **Create secret** panel.

  a. In the **Name** field, enter the name to be displayed in the list of certificates.

  b. Click the **Upload certificate** button to add a file with the Active Directory certificate.

  Base64-encoded X.509 certificate public keys are supported.

  c. If necessary, select the tags for the certificate from the **Tags** drop-down list.

  d. If necessary, enter a description of the certificate in the **Description** field.

  e. Then click the **Create** button.

  The certificate will be uploaded and displayed in the **Certificate** list.

> The **Certificate** field is optional if you have selected the **Insecure** TLS encryption type.

11. In the **Timeout in seconds** field, indicate the amount of time to wait for a response from the domain controller server.

    If multiple addresses are specified in the **URL** field, KUMA waits for a response from the first server for the specified time in seconds. If no response is received during that time, the solution attempts to connect to the next server. If none of the indicated servers responds during the specified amount of time, the connection will be terminated with an error.

12. In the **Base DN** field, enter the base distinguished name of the directory in which you need to run the search query.

13. In the **Custom AD account attributes** field, specify additional attributes to be used to enrich events.

    How to specify additional attributes

    Before configuring event enrichment using custom attributes, make sure that custom attributes are configured in AD.

    To enrich events with accounts using custom attributes:

    1. Add **Custom AD Account Attributes** in the LDAP connection settings.

       Default imported attributes from AD cannot be added as custom attributes. For example, if you add the standard `accountExpires` attribute as a custom attribute, KUMA returns an error when saving the connection settings.

       List of attributes imported from AD

       The following account attributes can be requested from Active Directory:

       - `accountExpires`
       - `badPasswordTime`
       - `cn`

- `company`
- `department`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `ipaUniqueID`
- `l`
- `mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (this attribute can be used for search during correlation)
- `mobile`
- `objectGUID` (this attribute always requested from Active Directory even if a user doesn't specify it)
- `objectSid`
- `physicalDeliveryOfficeName`
- `sAMAccountName`
- `sAMAccountType`
- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `userPrincipalName`
- `whenChanged`
- `whenCreated`

After you add custom attributes in the LDAP connection settings, the **LDAP attributes** drop-down list in the collector will be automatically appended with new attributes. Custom attributes are identified by a question mark next to the attribute name. If you added the same attribute for multiple domains, the attribute is listed only once in the drop-down list. You can view the domains by moving your cursor over the question mark. Domain names are displayed as links. If you click a link, the domain is automatically added to **LDAP accounts mapping** if it was not previously added.

If you deleted a custom attribute in the LDAP connection settings, delete the row containing the attribute from the collector's mapping table manually. Account attribute information in KUMA is updated each time you import accounts.

2. Import accounts.

3. In the collector, in the **LDAP mapping** table, define the rules for mapping KUMA fields to LDAP attributes.

4. Restart the collector.

   After the collector is restarted, KUMA begins enriching events with accounts.

14. Then click the **Create** button.

    If the tenant is deleted while creating a connection, the **New** button remains active, but an error message appears when you try to create a connection. The deleted tenant is displayed in the list of available tenants until you refresh the page by pressing the **F5** key.

The LDAP connection to Active Directory will be created and displayed in the **LDAP server integration** panel.

Account information from Active Directory will be requested immediately after the connection is saved, and then it will be updated at the specified frequency.

> If you want to use multiple LDAP connections simultaneously for one tenant, you need to make sure that the domain controller address indicated in each of these connections is unique. Otherwise, KUMA lets you enable only one of these connections. When checking the domain controller address, the application does not check whether the port is unique.

Creating a copy of an LDAP server connection

You can create an LDAP connection for another tenant by copying an existing connection. In this case, all settings of the original connection are duplicated in the newly created connection.

To copy an LDAP connection:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section and select the tenant for which you want to copy an LDAP connection.

2. Select a connection and click the **Add settings for a new tenant** button.

3. This opens the **LDAP server integration** window; in that window, in the **Tenant** drop-down list, select the tenant for which you want to create a copy of the connection.

4. Click the **Run import task** button.

5. Click the **Save** button.

   The new connection is created.

If you want to use multiple LDAP connections simultaneously for one tenant, you need to make sure that the domain controller address indicated in each of these connections is unique. Otherwise KUMA lets you enable only one of these connections. When checking the domain controller address, the application does not check whether the port is unique.

Changing an LDAP server connection

To change an LDAP server connection:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.

2. Select the tenant for which you want to change the LDAP server connection.

   The **LDAP server integration** panel will open on the right.

3. Click the LDAP server connection that you want to change.

   The window with the settings of the selected LDAP server connection opens.

4. Make the necessary changes to the settings.

5. Click the **Save** button.

   The LDAP server connection will be changed.

6. Restart the KUMA services that use LDAP server data enrichment for the changes to take effect.

Changing the data update frequency

KUMA queries the LDAP server to update account data. This occurs:

- Immediately after creating a connection.
- Immediately after changing the settings of an existing connection.
- According to a regular schedule every several hours. Every 12 hours by default.
- Whenever a user creates a task to update account data.

When querying LDAP servers, a task is created in the **Task manager** section of the KUMA web interface.

To change the schedule of KUMA queries to LDAP servers:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.
2. In the **LDAP server integration by tenant** window, select a tenant.

   The **LDAP server integration** window opens.
3. In the **Data refresh interval in hours** field, specify the required interval in hours. The default value is 12.

The query schedule will be changed.

Changing the data storage period

Received user account data is stored in KUMA for 90 days by default if information about these accounts is no longer received from the Active Directory server. After this period, the data is deleted.

After KUMA account data is deleted, new and existing events are no longer enriched with this information. Account information will also be unavailable in alerts. If you want to view information about accounts throughout the entire period of alert storage, you must set the account data storage period to be longer than the alert storage period.

To change the storage period for the account data:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.
2. In the **LDAP server integration by tenant** window, select a tenant.

   The **LDAP server integration** window opens.
3. In the **Data storage time** field, specify the number of days you need to store data received from the LDAP server.

The account data storage period is changed.

Starting account data update tasks

After a connection to an Active Directory server is created, tasks to obtain account data are created automatically. This occurs:

- Immediately after creating a connection.
- Immediately after changing the settings of an existing connection.
- Regularly at the specified interval, by default—every 12 hours.

You can import Active Directory account information for all connections or for individual connections of the required tenant.

To import data about Active Directory accounts for all LDAP connections of a tenant:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.
2. In the **LDAP server integration by tenant** table, select a tenant.

   The **LDAP server integration** panel will open on the right.
3. Click the **Run import task** button.

In the **Task Manager** section of the KUMA web interface, a task is added and started to import Active Directory account data for the selected tenant.

To import data about Active Directory accounts for one LDAP tenant connection:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.
2. In the **LDAP server integration by tenant** table, select a tenant.

   The **LDAP server integration** panel will open on the right.
3. Under **Connections**, select a connection to the LDAP server.
4. In the panel that opens, click the **Run import task** button.

In the **Task Manager** section of the KUMA web interface, a task is added and started to import Active Directory account data for the selected tenant connection.

Deleting an LDAP server connection

To delete LDAP connection to Active Directory:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **LDAP server** section.
2. In the **LDAP server integration by tenant** window, select a tenant.
3. Click the **Delete** button.
4. Confirm deletion of the connection.

The LDAP connection to Active Directory will be deleted.

Authentication using domain accounts

To learn more about the process of authentication in the solution web interface using Active Directory accounts, watch the video below, and then follow the step-by-step instructions.

https://www.youtube.com/watch?v=BoMtQVxYXh4

Authentication in the web interface using domain credentials involves the following steps:

1 Enabling domain authentication

Enable domain authentication. Domain authentication is disabled by default, and a domain connection is not configured.

2 Configuring a domain controller connection

The following connections are available:

- Active Directory (AD).
- Active Directory Federation Services (AD FS).
- FreeIPA

AD and AD FS connection settings can be configured simultaneously.

You can connect to one domain only.

3 Adding groups of user roles

You can add a domain group for each KUMA role. After being authenticated using their domain accounts, the users from this group get access to the web interface in accordance with their specified roles.

KUMA checks whether the user's group matches the specified filter in the following order of precedence of roles in the web interface: Junior analyst → Tier 1 analyst → Tier 2 analyst → Tenant administrator → General administrator. Upon the first match, the program assigns a role to the user and does not check any further. If a user matches two groups in the same tenant, the role with the highest privileges is assigned. If multiple groups are matched for different tenants, the user will be assigned the specified role in each tenant.

In the **Settings** → **Access** → **Domain Authentication** section, under **Administration groups**, the list of created groups of user roles will be displayed:

- Clicking a tenant name opens the list of roles and domain user groups associated with this tenant.
- Roles are sorted in descending order of seniority.
- No duplicate relations between user roles and domain user groups are created within a tenant. For example, if you copy relation *role 1, group 1* from tenant A to tenant B, in which the same relation already exists, a duplicate relationship is not created.

After their first authentication, all domain users gain access to the default space, which is specified in the **Access to spaces** section.

For successful authentication, the following conditions must be met:

- **FreeIPA**: when logging in to the system, the user must capitalize the domain name, for instance `user@FREEIPA.COM`.
- **AD/ADFS**: when logging in to the system, the user must specify UserPrincipalName in the login, for instance `user@domain.ru`.

After the first authentication of the user, information about this user is displayed in the **Settings** → **Access** → **Users** section. The **Login** and **Password** fields received from the domain cannot be edited. User roles are unavailable for editing. To change user roles, you need to change the links between roles and domain user groups. Changes to user roles are applied after repeated authentication of the user. The user continues working under the current roles until the current session expires.

If the user name or email address is changed in the domain account properties, these changes must be applied to the user account manually.

If users fail to authenticate in the KUMA web interface with their domain accounts after you completed all configuration steps, we recommend checking for the following:

- An email address is not indicated in the properties of the user account in Active Directory. If this is the case, an error message is displayed during the user's first authentication attempt and a KUMA account is not created.
- There is already an existing local KUMA account with the email address indicated in the domain account properties. If this is the case, the error message is displayed when the user attempts to perform authentication with the domain account.
- Domain authentication is disabled in the KUMA settings.
- An error occurred when entering the group of roles.
- The domain user name contains a space.

Enabling and disabling domain authentication

Domain authentication is disabled by default. To enable it, enable the **State** toggle switch. If you want to temporarily suspend domain authentication after configuring a connection, you can disable it in the KUMA web interface without deleting the previously defined values of settings. If necessary, you can enable authentication again at any time.

To enable or disable domain authentication of users in the KUMA web interface:

1. In the solution web interface, select **Settings** → **Access** → **Domain authentication**.
2. In the **Authorization type** drop-down list, select one of the options:
   - **AD/ADFS**.
   - **FreeIPA**
3. Do one of the following:
   - If you want to enable domain authentication, enable the **State** toggle switch.
   - If you want to disable domain authentication, disable the **State** toggle switch.
4. Click the **Save** button.

The selected settings will then be saved and applied.

Configuring connection between KUMA and Active Directory

You can connect only to one Active Directory domain. To do so, you must configure a connection to the domain controller.

To configure a connection to an Active Directory domain controller:

1. In the solution web interface, select **Settings** → **Access** → **Domain authentication**.
2. In the **Authorization type** drop-down list, select **AD/ADFS**.
3. Under **Active Directory (AD)**, enable the **State** toggle switch.
4. In the **Base DN** field, enter `DistinguishedName` of the root record to search for access groups in the Active Directory catalog service.
5. In the **URL** field, enter the address of the domain controller in the `<hostname or IP address of server>:<port>` format.

   > You can enter a comma-delimited list of addresses of domain controller servers for failover in case of unavailability. All of the specified servers must reside in the same domain.

6. If you want to use TLS encryption for the connection with the domain controller, select one of the following options from the **TLS mode** field:

   - **LDAPS**.

     When using LDAPS, an encrypted connection is immediately established over port 636.

   - **StartTLS**.

     When the STARTTLS command is used, first it establishes an unencrypted connection on port 389, then it sends an encryption request. If the STARTTLS command ends with an error, the connection is terminated.

     > Make sure that port 389 is open. Otherwise, a connection with the domain controller will be impossible.

   - **Insecure**.

     When using an encrypted connection, it is impossible to specify an IP address as a URL.

7. If you enabled TLS encryption at the previous step, select the previously created encryption certificate from the **Secret** drop-down list or add a new encryption certificate by selecting **Create new**:

   a. In the **Create secret** window, in the **Name** field, enter the name of the secret that will be displayed in the list after it is saved.

   b. Click the **Upload certificate** button.

   c. Specify the path to the previously created encryption certificate and click the **Open** button.

   d. Then click the **Create** button.

   The secret is uploaded and becomes available for selection in the **Secret** drop-down list.

8. In the **Timeout in seconds** field, specify the time to wait for a response from the domain controller server. The default value is 0.

   If multiple addresses are specified in the **URL** field, the solution waits for a response from the first server for the specified number of seconds. If no response is received during that time, the solution attempts to connect to the next server. If none of the indicated servers responds during the specified amount of time, the connection will be terminated with an error.

9. In the **Check connection** field, click **Check** button to test the connection with the domain controller.

   The system tests the connection with the domain and returns a notification with the test results. The system does not check if the users can log in or if the user group is configured correctly.

10. If you want to configure domain authentication for a user with the General administrator role, use the **General administrators group** field to specify `DistinguishedName` of the FreeIPA group the user is a member of. Since additional roles for the General administrator are activated automatically, you do not need to add them individually.

    > If multiple groups are specified for a user in the same tenant, the role with the highest-level permissions is used, with additional roles, if additional roles are assigned.

    Filter input example: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

11. Click the **Save** button.

A connection with the Active Directory domain controller is now configured.

Configuring connection between KUMA and Active Directory Federation Services

Configuring a connection between KUMA and Active Directory Federation Services involves the following steps:

1 Creating a connection group

The AD FS role must already be configured on the server.

1. In **Server Manager**, in the **Tools** menu, select **ADFS Management**.
2. Select the **Application groups** section and in the **Actions** section click **Add Application Group**.
3. In the opened window, in the **Welcome** section **Name** field, specify the name of the new connection group.

   Example

   ```
   new-application-group
   ```

4. In the **Template** field, in the **Client-Server applications** group, select **Native application accessing a web API**.
5. Click **Next**.

   In the **Native application** section that opens, **Name** and **Client Identifier** fields are filled in automatically. Specify the value of the **Client Identifier** field in the **Client Identifier** field in KUMA, when configuring domain authentication.

6. In the **Redirect URI** field, enter the URI for redirection from AD FS with the `/sso-callback` substring, and click **Add**.

   Example

   ```
   https://adfs.example.com:7220/sso-callback
   ```

7. Click **Next**.
8. In the displayed section, that opens, in the **Identifiers** field, add the trusted party ID and click **Add**.

   It can be any arbitrary value. Example: `test-demo`.

   Specify the value of the **Identifier** field in KUMA, in the **Relying party identifiers** field, when configuring domain authentication.

9. Click **Next**.
10. In the displayed section, select the **Permit everyone** policy.
11. Click **Next**.

    In the **Configure Application Permissions** section that opens, the **Client application** field is filled in automatically.

12. In the **Permitted scopes** field, select the check box for **allatclaims** and **openid** options.
13. Click **Next**.

14. In the **Summary** section that opens, check the settings.

15. If the settings are correct and you are ready to add a group, click **Next**.

    This will add a new group. You can proceed to configure the rules for the created group.

❷ Adding rules for a connection group

The AD FS role must already be configured on the server.

1. In **Server Manager**, in the **Tools** menu, select **ADFS Management**.

2. In AD FS, select the **Application groups** section, and select the required connection group from the list in the window that opens.

   Example
   ```
   new-application-group
   ```

3. In the **Application groups** window, in the **Actions** section, click **Properties**.

4. In the **new-application-group Properties** window that opens, in the **Applications** section, double-click **new-application-group - Web API**.

5. In the opened window, go to the **Issuance Transform Rules** tab and click **Add rule**.

6. In the opened window, in the **Choose Rule Type** section, select **Send LDAP Attributes as Claims** from the drop-down list.

7. Click **Next**.

8. In the **Configure Claim Rule** section, specify the rule name in the **Claim rule name** field.

   Example
   ```
   rule-name-01
   ```

9. In the **Attribute store** drop-down list, select **Active directory**.

10. In the **Mapping of LDAP attributes to outgoing claim types** field, map the following fields:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	UserPrincipalName
Display-Name	displayName
E-Mail-Addresses	Mail
Is-Member-Of-DL	MemberOf

11. Click **Finish**.

12. Return to the **new-application-group - Web API Properties** window, switch to the **Issuance Transform Rules** tab and click **Add rule**.

13. In the opened window, in the **Choose Rule Type** section, select **Send claims using a custom rule** from the drop-down list.

14. Click **Next**.

15. In the **Configure Claim Rule** section, specify the rule name in the **Claims rule name** field.

Example

```
rule-name-02
```

16. In the **Custom rule** field, specify the following settings:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]=> issue(store = "Active Directory", types = ("ObjectGUID"), query = ";ObjectGUID;{0}", param =
c.Value);
```

17. Click **Finish**.

    The **new-application-group – Web API Properties** window is opened with the **Issuance Transform Rules**tab selected.

18. To apply the rules, on the **Issuance Transform Rules** tab that opens, click **Apply** or **OK**.

The configuration of groups and rules in AD FS is complete. You can proceed to configure domain authentication in KUMA.

3 Configuring domain authentication in KUMA

You can connect to only one AD FS domain.

1. In the solution web interface, select **Settings** → **Access** → **Domain authentication**.

2. In the **Authorization type** drop-down list, select **AD/ADFS**.

3. Under **Active Directory Federation Services (ADFS)**, enable the **State** toggle switch.

4. In the **Client ID** field, copy the KUMA ID from the **Client ID** field in AD FS.

5. In the **Relying party identifier** field, copy the KUMA ID from the **Relying party identifiers** field in the AD FS.

6. In the **Connect Metadata URI** field, copy the URI from the **Connect Metadata URI** field. The URI consists of the host of the AD FS (`https://adfs.example.com`) and the endpoint configuration parameter (`/adfs/.well-known/openid-configuration`).

   Example

   ```
   https://adfs.example.com/adfs/.well-known/openid-configuration
   ```

7. Enter the **Redirect URL** from the **Redirect URL** field in the AD FS. The value of the **Redirect URL** field in the AD FS is defined when the Application group is configured. In the AD FS, you need to indicate the KUMA FQDN and the `</sso-callback>` substring. In KUMA, the URL must be indicated without a substring, for example: `https://kuma-example:7220`.

   In a distributed installation with KUMA Core in a Raft cluster, you need to configure the balancer and then specify its FQDN. For example, in the AD FS settings, you need to specify `https://kuma-load-balancer.com:7220</sso-callback>`, and in KUMA, in the **Redirect URL** field, you need to specify `https://kuma-load-balancer.com:7220`.

8. If you want to configure domain authentication for a user with the General administrator role, use the **General administrators group** field to specify `DistinguishedName` of the FreeIPA group the user is a member of. Since additional roles for the General administrator are activated automatically, you do not need to add them individually.

   > If multiple groups are specified for a user in the same tenant, the role with the highest-level permissions is used, with additional roles, if additional roles are assigned.

   Filter input example: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

9. Click the **Save** button.

A connection with the Active Directory Federation Services domain controller is now configured.

After configuration, the **Sign in via ADFS** button appears on the KUMA login page. The **Sign in via ADFS** button is hidden on the KUMA login page in the following conditions:

- The **FreeIPA** option is selected in the **Authorization type** drop-down list.
- The **AD/ADFS** option is selected in the **Authorization type** drop-down list and the settings for AD FS are not specified or the **State** toggle switch is enabled for AD FS settings.

> If, when trying to log in to KUMA via AD FS, the user gets a pop-up message (`Access denied` or `Insufficient privileges`), click the **Reset certificate** button. A new certificate will be generated automatically.

Configuring connection between KUMA and FreeIPA

You can connect only to one FreeIPA domain. To do so, you must configure a connection to the domain controller.

To configure a connection to a FreeIPA domain controller:

1. In the solution web interface, select **Settings** → **Access** → **Domain authentication**.
2. In the **Authorization type** drop-down list, select **FreeIPA**.
3. Under **FreeIPA**, enable the **State** toggle switch.
4. In the **Base DN** field, enter `DistinguishedName` of the root record to search for access groups in the FreeIPA catalog service. Record format: `dc=example,dc=com`.
5. In the **URL** field, enter the address of the domain controller in the `<hostname or IP address of server>:<port>` format.

   > You can enter a comma-delimited list of up to three addresses of domain controller servers for failover in case of unavailability. All of the specified servers must reside in the same domain.

6. If you want to use TLS encryption for the connection with the domain controller, select one of the following options from the **TLS mode** field:

   - **LDAPS**.

     When using LDAPS, an encrypted connection is immediately established over port 636.

   - **StartTLS**.

     When the STARTTLS command is used, first it establishes an unencrypted connection on port 389, then it sends an encryption request. If the STARTTLS command ends with an error, the connection is terminated.

     > Make sure that port 389 is open. Otherwise, a connection with the domain controller will be impossible.

   - **Insecure**.

     When using an encrypted connection, it is impossible to specify an IP address as a URL.

7. If you enabled TLS encryption at the previous step, select the previously created encryption certificate from the **Secret** drop-down list or add a new encryption certificate by selecting **Create new**:

   a. In the **Create secret** window, in the **Name** field, enter the name of the secret that will be displayed in the list after it is saved.

   b. Click the **Upload certificate** button.

   c. Specify the path to the previously created encryption certificate and click the **Open** button.

   d. Then click the **Create** button.

   The secret is uploaded and becomes available for selection in the **Secret** drop-down list.

8. In the **Timeout in seconds** field, specify the time to wait for a response from the domain controller server. The default value is 0.

   If multiple addresses are specified in the **URL** field, the solution waits for a response from the first server for the specified number of seconds. If no response is received during that time, the solution attempts to connect to the next server. If none of the indicated servers responds during the specified amount of time, the connection will be terminated with an error.

9. In the **Custom integration secret** drop-down list, select a previously created encryption certificate or add a new encryption certificate by selecting **Create new**:

   a. In the **Create secret** window, in the **Name** field, enter the name of the secret that will be displayed in the list after it is saved.

   b. In the **User** field, enter `DistinguishedName` in the following format: `uid=admin,cn=users,cn=accounts,dc=ipa,dc=test`.

   c. Enter a **Password**.

   d. Then click the **Create** button.

   The secret is uploaded and becomes available for selection in the **Custom integration secret** drop-down list.

10. In the **Check connection** field, click **Check** button to test the connection with the domain controller.

    The system tests the connection with the domain and returns a notification with the test results. The system does not check if the users can log in or if the user group is configured correctly.

11. If you want to configure domain authentication for a user with the General administrator role, use the **General administrators group** field to specify `DistinguishedName` of the FreeIPA group the user is a member of. Since additional roles for the General administrator are activated automatically, you do not need to add them individually.

    > If multiple groups are specified for a user in the same tenant, the role with the highest-level permissions is used, with additional roles, if additional roles are assigned.

    Filter input example: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

12. Click the **Save** button.

A connection with the FreeIPA domain controller is now configured.

Managing links between roles and domain user groups

This article describes how to add, copy, or delete links between roles and domain user groups.

Adding a link between roles and domain user groups

To add a link between roles and domain user groups:

1. In the web interface, open **Settings** → **Access** → **Domain authentication**.

2. Under **Administration groups**, click **Add group**.

3. In the **Tenant** drop-down list, select the tenant of the users for whom you want to configure domain authentication.

4. In the **Roles** drop-down list, select the required user roles.

   A filter field appears for each selected role. In the filter field for each role, enter the full path to the domain group whose users can authenticate by using their domain credentials. Example of group specification: `CN=KUMA team`, `OU=Groups`, `OU=Clients`, `DC=test`, `DC=domain`.

   If no filter is specified for a role, this means that conditions for creating an account via domain authentication are not specified for that role. Domain authentication with that role is impossible.

   Once users authenticate using their domain accounts for the first time, domain user cards are created in the **Settings** → **Access** → **Users** section.

   For a domain user, the ability to change the main roles (General administrator, Tenant administrator, Tier 2 analyst, Tier 1 analyst, Junior analyst) is blocked in the user card, while additional roles can be added or removed (e.g., Access to CII, Interaction with NCIRCC, Read shared resources), including management of additional role assignment to tenants.

   Roles assigned in the **Settings** → **Access** → **Domain authentication** section and in the user card supplement each other.

   For the General administrator, additional roles are activated automatically, therefore you do not need to add them separately. If the General administrator role was assigned to a domain user, and the General administrator role was subsequently revoked, additional roles must be reassigned in the user card in the **Settings** → **Access** → **Users** section.

> You can specify only one domain group in the group settings for each role. If you want to connect a role with multiple domain groups, you need to repeat steps 2 to 4 for each group while specifying the same tenant.

5. If necessary, repeat steps 2–4 for each tenant for which you want to configure domain authentication.

6. Then click the **Add** button.

   Links between roles and domain user groups are added. The defined settings will be applied the next time the user logs in to the web interface.

Copying links between roles and domain user groups

To copy links between roles and domain user groups:

1. In the web interface, open **Settings** → **Access** → **Domain authentication**.

2. In the **Administration groups** settings section, select the check boxes next to the names of tenants for which the link between the role and the domain user group is created.

3. Click the **Copy to clipboard** button.

4. In the window **Copy to tenant** that opens, select one or more tenants for which you want to copy the selected links.

5. Click the **Copy** button.

   Copies of the links are displayed in the list.

Deleting links between roles and domain user groups

To delete links between roles and domain user groups:

1. In the web interface, open **Settings** → **Access** → **Domain authentication**.

2. In the **Administration groups** settings section, select the check boxes next to the names of tenants for which the link between the role and the domain user group is created.

3. Click the **Delete** button.

   The selected links between roles and domain user groups are deleted from the list.

NCIRCC integration

In the KUMA web interface, you can create a connection to the National Computer Incident Response & Coordination Center Incidents (hereinafter referred to as "NCIRCC"). This will let you export incidents registered by KUMA to NCIRCC.

All settings specified when configuring the integration will be automatically sent to the form for sending data to NCIRCC.

Data in KUMA and NCIRCC is synchronized every 5–10 minutes.

To establish a connection to NCIRCC:

1. In the web interface, open the **Settings** → **Integrations** → **NCIRCC** section.

2. Use the **Status** toggle switch to enable the integration.

   The integration is disabled by default.

3. In the **URL** field, enter the URL for accessing NCIRCC.

4. In the **Tenant** drop-down list, select a tenant for messages from NCIRCC.

5. In the **Token** drop-down list, create or select a secret with the API token that was issued to your organization for connecting to NCIRCC:

   If you want to create a new secret:

   a. Click **Create** and in the **Create secret** window, specify the following settings:

      - In the **Name** field, enter a unique name for the secret you are creating. The name must contain 1 to 128 Unicode characters.

      - In the **Token** field, enter a token that was issued to your organization for connection to NCIRCC.

      - If necessary, select the tags for the created secret from the **Tags** drop-down list.

      - If required, add a description for the secret in the **Description** field. You can add up to 256 Unicode characters.

   b. Click **Create**.

   The secret containing the token for connecting to NCIRCC is created. It is stored under **Resources** → **Resources** → **Secrets** and is owned by the Main tenant.

6. In the **Company scope** drop-down list, select the required value.

7. In the **Company name** field, specify the name of the company for which you are configuring the integration.

8. In the **Location** drop-down list, specify the location of your company.

9. In the **Root CA** drop-down list, select or create a secret.

   If you want to create a new secret:

   a. Click the **Create** button and specify the following settings:

      - In the **Name** field, enter a unique name for the secret you are creating. The name must contain 1 to 128 Unicode characters.

      - For the **Certificate file** parameter, click the **Upload certificate** button and select the certificate of the intermediate certification authority that is uploaded and installed on the KUMA Core server.

        Download and install the certificate of the intermediate certification authority.

To install and trust the certificate of the intermediate certification authority on the KUMA Core server:

1. Follow the link from the user profile to NCIRCC, for example, `https://lk.cert.gov.ru`.

2. Right-click to call up the **View site details** context menu to the left of the link in the address bar.

   - If you are using an encrypted connection, select **Connection is secure** and in the drop-down list under **Certificate is valid**, click **Show certificate**.

   - If you are using an unencrypted connection, click **Certificate details**.

   Depending on your browser, the position of the menu and the order of items may differ.

3. In the **Certificate Viewer** window, under **Issued By**, in the **Common Name (CN)** field you can find the name of the relevant certificate, for example, `GlobalSign GCC R6 AlphaSSL CA 2023`.

   Remember the name of the certificate because you will need to download it at the next step.

4. Follow the link https://support.globalsign.com/ca-certificates/intermediate-certificates/alphassl-intermediate-certificates, find the certificate from step 3, and click **View as BASE64**.

5. Paste the displayed certificate strings into a file and add the file with the certificate strings as the secret in KUMA.

6. After installing the certificate, restart the KUMA Core server.

   The certificate is installed and you can proceed with configuring the integration.

- If necessary, select the tags to label the certificate from the **Tags** drop-down list.

- If required, add a description for the secret in the **Description** field. You can add up to 256 Unicode characters.

b. Click **Create**.

The secret with the certificate of the intermediate certification authority is created. It is stored in the **Resources** → **Resources** → **Secrets** section and is owned by the main tenant.

10. If necessary, under **Proxy**, create or select an existing proxy server that should be used when connecting to NCIRCC.

11. Specify the NCIRCC response timeout in seconds.

12. If necessary, specify the tax ID (INN), operator address, and email address for sending notification information.

13. Click **Save**.

14. If you want to verify that a connection to NCIRCC is established, click the **Check connection** button.

KUMA is now integrated with NCIRCC. You can export incidents to NCIRCC.

If the `https://lk.cert.gov.ru/api/v2/incidents? x509: certificate signed by unknown authority error` is returned when you configure integration with NCIRCC, download and install the certificate of the intermediate certification authority on the KUMA Core server.

Integration with the Security Orchestration Automation and Response Platform (SOAR)

Security Orchestration, Automation and Response Platform (hereinafter referred to as SOAR) is a software platform used for automation of monitoring, processing, and responding to information security incidents. It aggregates cyberthreat data from various sources into a single database for further analysis and investigation to facilitate incident response capabilities.

SOAR can be integrated with KUMA. After configuring integration, you can perform the following tasks in SOAR:

- Request information about alerts from KUMA. In SOAR, *incidents* are created based on received data.
- Send requests to KUMA to close alerts.

Integration is implemented by using the KUMA REST API. On the Security Vision IRP side, integration is carried out by using the preconfigured **Kaspersky KUMA** connector. Contact your SOAR vendor to learn more about the methods and conditions for obtaining a **Kaspersky KUMA** connector.

Managing SOAR incidents

SOAR incidents generated from KUMA alert data can be viewed in SOAR under **Incidents** → **Incidents (2 lines)** → **All incidents (2 lines)**. Events related to KUMA alerts are logged in each SOAR incident. Imported events can be viewed on the **Response** tab.

KUMA alert imported into SOAR as an incident

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Id: 1781339 Тип: Инцидент (2 линии)

Дата и время создания: 16:06:07 14.04.2022

Доступные базовые действия:

Взять в работу

Доступные действия по реагированию:

Общая информация

Наименование: Обнаружен инцидент Test Correlation rule у Main

Описание: Обнаружен алерт [illegible] вида "Test Correlation rule" на инфраструктуре Main в 13:05:56 14.04.2022. Адрес источника - [illegible], Адрес назначения - [illegible]

Информация об источнике

IP-адрес источника: [illegible]

Порт источника: [illegible]

Имя узла источника:

Имя пользователя:

Активы источника

Информация о назначении

IP-адрес назначения: [illegible]

Порт назначения:

Имя узла назначения: [illegible]

Имя пользователя назначения:

Активы назначения

Обработка инцидента

Приоритет: Низкий

Группа исполнения: Мониторинг инцидентов КБ

Исполнитель:

Этап обработки: Ожидание взятия в работу

Статус: Новый

Ложное срабатывание:

Вердикт:

Рекомендации:

Обработка инцидента(SLA)

Дата и время создания: 16:06:07 14.04.2022

Дата и время взятия в работу:

Дата и время закрытия:

Сохранить | Сохранить и выйти | Отмена

Security Vision IRP incident that was created based on KUMA alert

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Jira

Идентификатор Jira:

Статус Jira:

Переписка с пользователем

Почтовая переписка:

Вложения почтовой переписки:

Обогащение из AD

Информация о пользователе из AD:

Координата X:

Координата Y:

События QRadar

Событие	Время события	Имя пользователя	IP-адрес источника	Порт источника	IP-адрес назначения
service started	2022-04-14T16:05:51.000+03:00		[illegible]	[illegible]	[illegible]
service started	2022-04-14T16:05:56.000+03:00		[illegible]	[illegible]	[illegible]

Events from KUMA alert that were imported to Security Vision IRP

Configuring integration in KUMA

To configure KUMA integration with SOAR, you must configure authorization of API requests in KUMA. To do so, you need to create a token for the KUMA user on whose behalf the API requests will be processed on KUMA side.

A token can be generated in your account profile. Users with the General Administrator role can generate tokens in the accounts of other users. You can always generate a new token.

To generate a token in your account profile:

1. In the KUMA web interface, click the user account name in the lower-left corner of the window and click the **Profile** button in the opened menu.

   The **User** window with your user account parameters opens.

2. Click the **Generate token** button.

3. Copy the generated token displayed in the opened window. You will need it to configure SOAR.

   When the window is closed, the token is no longer displayed. If you did not copy the token before closing the window, you will have to generate a new token.

The generated token must be specified in the SOAR connector settings.

Configuring integration in SOAR

Configuration of integration in SOAR consists of importing and configuring a connector. If necessary, you can also change other SOAR settings related to KUMA data processing, such as the data processing schedule and worker.

For more detailed information about configuring SOAR, please refer to the product documentation.

Importing and configuring a connector

Adding a connector to SOAR

Integration of SOAR and KUMA is performed using the **Kaspersky KUMA** connector. Contact your SOAR vendor to learn more about the methods and conditions for obtaining a **Kaspersky KUMA** connector.

*To import the **Kaspersky KUMA** connector to SOAR:*

1. In SOAR, open the **Settings** → **Connectors** → **Connectors** section.

   A list of connectors added to SOAR is displayed.

2. At the top of the screen, click the import button and select the ZIP archive containing the **Kaspersky KUMA** connector.

The connector is imported into SOAR and is ready to be configured.

Configuring a connector for a connection to KUMA

To use a connector, you need to configure its connection to KUMA.

*To configure a connection to KUMA in SOAR using the **Kaspersky KUMA** connector:*

1. In SOAR, open the **Settings** → **Connectors** → **Connectors** section.

   A list of connectors added to your SOAR is displayed.

2. Select the **Kaspersky KUMA** connector.

   The general settings of the connector will be displayed.

3. Under **Connector settings**, click the **Edit** button.

   The connector configuration will be displayed.

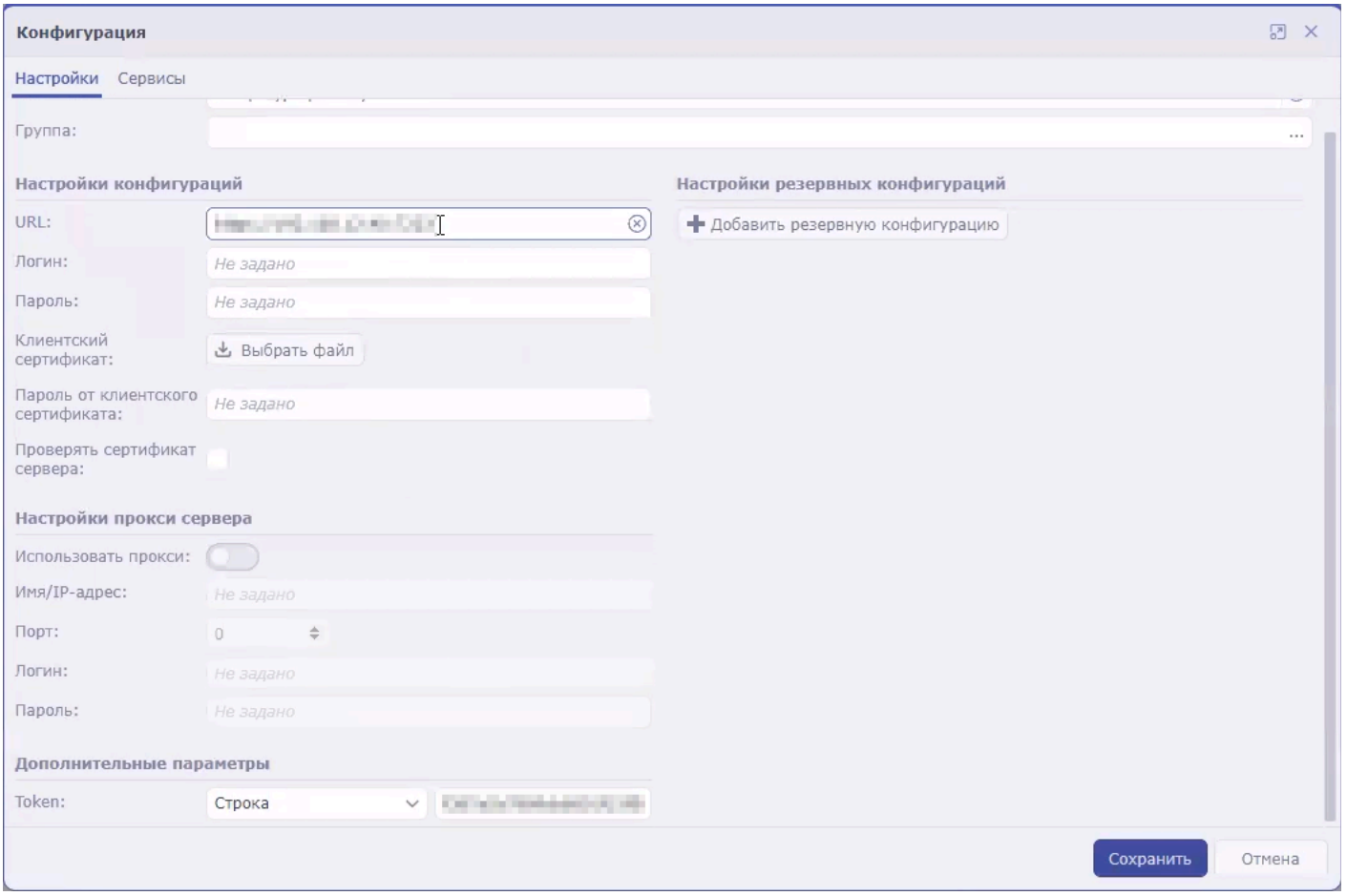
4. In the **URL** field, specify the address and port of KUMA, for example:

   ```
   kuma.example.com:7223
   ```

5. In the **Token** field, specify KUMA user API token.

The connection to KUMA is configured in the SOAR connector (click the links below for an image).

Security Vision IRP connector settings



Security Vision IRP connector settings

Configuring commands for interaction with KUMA in the SOAR connector

You can use SOAR to receive information about KUMA alerts (referred to as *incidents* in SOAR terminology) and send requests to close these alerts. To perform these actions, you need to configure the appropriate commands in the SOAR connector.

The instructions below describe how to add commands to receive and close alerts. However, if you need to implement more complex logic of interaction between SOAR and KUMA, you can similarly create your own commands containing other API requests.

To configure a command to receive alert information from KUMA:

1. In SOAR, open the **Settings** → **Connectors** → **Connectors** section.

   A list of connectors added to SOAR is displayed.

2. Select the **Kaspersky KUMA** connector.

   The general settings of the connector will be displayed.

3. Click the **+Command** button.

   The command creation window opens.

4. Specify the command settings for receiving alerts:

   - In the **Name** field, enter the command name: `Receive incidents`.
   - In the **Request type** drop-down list, select **GET**.
   - In the **Called method** field, enter the API request to search for alerts:

     ```
     api/v1/alerts/?withEvents&status=new
     ```

   - Under **Request headers**, in the **Name** field, indicate `authorization`. In the **Value** field, indicate **Bearer <token>**.
   - In the **Content type** drop-down list, select **application/json**.

5. Save the command and close the window.

The connector command is configured. When this command is executed, the SOAR connector queries KUMA for information about all alerts with the **New** status and all events related to those alerts. The received data is sent to the SOAR processor, which uses it to create SOAR incidents. If new data appears in an alert that has been already imported into SOAR, incident information is updated in SOAR.

To configure a command to close KUMA alerts:

1. In SOAR, open the **Settings** → **Connectors** → **Connectors** section.

   A list of connectors added to SOAR is displayed.

2. Select the **Kaspersky KUMA** connector.

   The general settings of the connector will be displayed.

3. Click the **+Command** button.

   The command creation window will be displayed.

4. Specify the command settings for receiving alerts:

   - In the **Name** field, enter the command name:

     ```
     Closing the incident
     ```

   - In the **Request type** drop-down list, select **POST**.

   - In the **Called method** field, enter API request to close an alert:

     ```
     api/v1/alerts/close
     ```

   - In the **Request** field, enter the contents of the sent API request:

     ```
     {"id":"<Alert ID>","reason":"responded"}
     ```

     You can create multiple commands for different reasons to close alerts, such as [responded, incorrect data, and incorrect correlation rule](#).

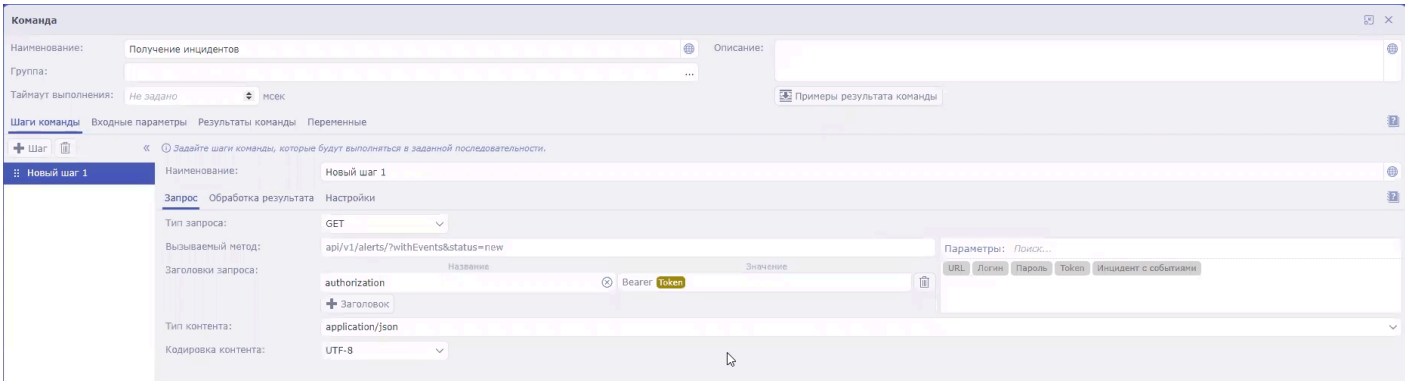
   - Under **Request headers**, in the **Name** field, indicate `authorization`. In the **Value** field, indicate **Bearer <token>**.

   - In the **Content type** drop-down list, select **application/json**.

5. Save the command and close the window.

   The connector command is configured (click the links below for an image). When this command is executed, the incident is closed in SOAR and the corresponding alert is closed in KUMA.

Creating commands in SOAR



Creating commands in SOAR

After the SOAR connector is configured, KUMA alerts are sent to the platform as SOAR incidents. Then you need to [configure incident handling in SOAR](#) based on the security policies of your organization.

Configuring the handler, schedule, and worker process

SOAR handler

The SOAR handler receives information about KUMA alerts from the SOAR connector and uses the information to create SOAR incidents. A predefined **KUMA (Incidents)** handler is used for processing data. The settings of the **KUMA (Incidents)** handler are available in SOAR under **Settings** → **Event processing** → **Event handlers**:

- You can view the rules for processing KUMA alerts in the handler settings on the **Normalization** tab.
- You can view the actions available when creating new objects in the handler settings on the **Actions** tab for creating objects of the **Incident (2 lines)** type.

Handler run schedule

The connector and handler are started according to a predefined **KUMA** schedule. This schedule can be configured in SOAR under **Settings** → **Event processing** → **Schedule**:

- Under **Connector settings**, you can configure the settings for starting the connector.
- Under **Handler settings**, you can configure the settings for starting the handler.

SOAR workflow

The life cycle of SOAR incidents created based on KUMA alerts follows the preconfigured **Incident processing (2 lines)** worker. The worker can be configured in SOAR under **Settings** → **Workers** → **Worker templates**: select the **Incident processing (2 lines)** worker and click the transaction or state that you need to change.

Integration with KICS for Networks and KATA

Kaspersky Industrial CyberSecurity for Networks (hereinafter referred to as "KICS for Networks") is an application designed to protect the industrial enterprise infrastructure from information security threats, and to ensure uninterrupted operation. The application analyzes industrial network traffic to identify deviations in the values of process parameters, detect signs of network attacks, and monitor the operation and current state of network devices.

Kaspersky Anti Targeted Attack (hereinafter referred to as KATA) is an application designed for protection of corporate IT infrastructure and early detection of threats such as zero-day attacks, targeted attacks, and advanced persistent threats.

KICS for Networks or KATA can be integrated with KUMA. After configuring integration, you can perform the following tasks in KUMA:

- Import asset information from KICS for Networks or KATA to KUMA.

  Import of asset information from KATA version 7.1 is available only in KUMA version 4.0 and later.

- Send asset status change commands from KUMA to KICS for Networks or KATA.

Unlike KUMA, KICS for Networks and KATA refers to assets as devices.

The integration of KICS for Networks or KATA and KUMA must be configured on both sides:

1. In KICS for Networks or KATA, you need to create a KUMA connector and save the communication data package of this connector.

   You can configure the integration on the side of KICS for Networks 4.0 or later as well as on the side of KATA 7.0 and later versions. Configuring the integration on either side allows correctly transmitting asset and event information to KUMA.

2. In KUMA, the communication data package of the connector is used to create a connection to KICS for Networks or KATA.

The integration described in this section applies to importing asset information. KICS for Networks or KATA can also be configured to send events to KUMA. To do so, you need to create a SIEM/Syslog connector in KICS for Networks or KATA, and configure a collector on the KUMA side.

Configuring integration in KICS for Networks or KATA

Integration can be configured on the side of KICS for Networks version 4.0 or on the side of KATA 7.0 or a later version For the import of data and events to work correctly, you must use the KUMA connector and the communication data package created in the appropriate system.

We recommend configuring integration of KICS for Networks or KATA with KUMA after ending Process Control rules learning mode. For more details, please refer to the KICS for Networks documentation.

On the KICS for Networks or KATA side, integration configuration consists of creating a *KUMA-type connector*. In KICS for Networks and KATA, connectors are specialized application modules that enable KICS for Networks or KATA to exchange data with recipient systems, including KUMA. For more details on creating connectors, please refer to the KICS for Networks documentation.

When a connector is added to KICS for Networks or KATA, a *communication data package* is automatically created for this connector. A communication data package is an encrypted configuration file for connecting to KICS for Networks or KATA that is used when configuring integration on the KUMA side.

Configuring integration in KUMA

We recommend configuring integration of KICS for Networks or KATA with KUMA after ending Process Control rules learning mode. For more details, please refer to the KICS for Networks documentation.

To configure integration with KICS for Networks or KATA in KUMA:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **KICS/KATA** section.

   This opens the **KICS/KATA integration by tenant** window.

2. Click the **Add settings for a new tenant** button.

3. This opens a window; in that window, specify the following KICS for Networks or KATA integration settings:

   - Turn on the **State** toggle switch. The toggle switch is turned on by default.

   - In the **Tenant** drop-down list, select a tenant for the integration with KICS for Networks or KATA.

   - Enable the **Enable responses** toggle switch to be able to change the statuses of KICS for Networks or KATA assets using KUMA response rules.

4. In the area with the **Connections** table, add a new connection by clicking the **+ Add** button.

5. This opens the **Create connection** window; in that window, manage the following settings:

   - Turn on the **State** toggle switch. The toggle switch is turned on by default.

   - In the **Communication data package** field, click the add (+) icon and select the communication data package of the connector that was created in KICS for Networks or KATA when creating a connector for the KUMA connection.

   - In the **Communication data package password** field, enter the password set for the communication data package.

   - In the **API version** field, specify the API version used by KICS for Networks or KATA. The default value is `Auto` (version 4.0).

6. Click **Save**.

   The created connection is automatically displayed in the table of connections of the selected tenant.

7. If necessary, add more connections within the same tenant.

8. In the **KICS/KATA integration by tenant** window, click **Add**.

Integration with KICS for Networks or KATA is configured in KUMA. You can view the ID of the node on which the KICS for Networks or KATA connector will run by clicking the link with its IP address.

Enabling and disabling integration with KICS for Networks or KATA

To enable or disable KICS for Networks or KATA integration for a tenant:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **KICS/KATA** section.

   This opens the **KICS/KATA integration by tenant** window.

2. Do one of the following:

   - Use the **Status** toggle switch to enable or disable the integration for the tenant.

   - Click the **Add settings for a new tenant** button to open a window and in that window, use the **State** toggle switch to enable or disable the integration for the tenant, and then save the changes.

Changing the data update frequency

KUMA queries KICS for Networks or KATA to update its asset information. This occurs:

- Immediately after creating a new integration.
- Immediately after changing the settings of an existing integration.
- According to a regular schedule every several hours. This occurs every 3 hours by default.
- Whenever a user creates a task for updating asset data.

When querying KICS for Networks or KATA, a task is created in the **Task manager** section of the KUMA web interface.

To edit the schedule for importing information about KICS for Networks or KATA assets:

1. In the KUMA web interface, open the **Settings** → **Integrations** → **KICS/KATA** section.
2. Select the relevant tenant.

   This opens the **KICS/KATA integration by tenant** window.
3. In the **Data refresh interval in hours** field, specify the data update interval in hours. The default value is 3.
4. Save your changes.

The import schedule has been changed.

Special considerations when importing asset information from KICS for Networks or KATA

Regardless of which side the integration is initiated from (KICS for Networks or KATA), the import of assets and vulnerabilities into KUMA is performed in accordance with standard rules, and IDs are preserved.

Importing assets

Assets are imported according to the asset import rules. Only assets with the **Authorized** and **Unauthorized** statuses are imported.

KICS for Networks and KATA assets are identified by a combination of the following parameters:

- IP address of the KICS for Networks or KATA instance with which the integration is configured.
- KICS for Networks or KATA connector ID is used to configure the integration.
- ID assigned to the asset (or "device") in the KICS for Networks or KATA instance.

Importing vulnerability information

When importing assets, KUMA also receives information about active vulnerabilities in KICS for Networks or KATA. If a vulnerability has been flagged as Remediated or Negligible in KICS for Networks or KATA, the information about this vulnerability is deleted from KUMA during the next import.

Information about asset vulnerabilities is displayed in the localization language of KICS for Networks or KATA in the **Asset details** window in the **Vulnerabilities** settings block.

> In KICS for Networks or KATA, vulnerabilities are referred to as *risks* and are classified into several types. All types of risks are imported into KUMA.

Imported data storage period

If information about a previously imported asset is no longer received from KICS for Networks or KATA, the asset is deleted after 30 days.

Changing the status of a KICS for Networks or KATA asset

After configuring integration, you can change the statuses of KICS for Networks or KATA assets from KUMA. Statuses can be changed either automatically or manually.

Asset statuses can be changed only if you enabled a response in the settings for connecting to KICS for Networks or KATA.

Manually changing the status of a KICS for Networks or KATA asset

Users with the General administrator, Tenant administrator, and Tier 2 analyst roles can manually change the statuses of assets imported from KICS for Networks or KATA in the tenants available to them.

To manually change a KICS for Networks or KATA asset status:

1. In the **Assets** section of the KUMA web interface, click the asset that you want to edit.

   The **Asset details** area opens in the right part of the window.

2. In the **Status in KICS/KATA** drop-down list, select the status that you want to assign to the KICS for Networks or KATA asset. The *Authorized* or *Unauthorized* statuses are available.

The asset status is changed. The new status is displayed in KICS for Networks or KATA and in KUMA.

Automatically changing the status of a KICS for Networks or KATA asset

Automatic changes to the statuses of KICS for Networks or KATA assets are implemented using response rules. The rules must be added to the correlator, which will determine the conditions for triggering these rules.

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (hereinafter also referred to as "ASAP") is an online learning platform that allows users to learn the rules of information security and threats related to it in their daily work, as well as to practice using real examples.

ASAP can be integrated with KUMA. After configuring integration, you can perform the following tasks in KUMA:

- Change user learning groups.
- View information about the courses taken by the users and the certificates they received.

Integration between ASAP and KUMA includes configuring API connection to ASAP. The process takes place in both solutions:

1. In ASAP, create an authorization token and obtain an address for API requests.
2. In KUMA, specify the address for API requests in ASAP, add an authorization token for API requests, and specify the email address of the ASAP administrator to receive notifications.

Creating a token in ASAP and getting a link for API requests

In order to be authorized, the API requests from KUMA to ASAP must be signed by a token created in ASAP. Only the company administrators can create tokens.

Creating a token

To create a token:

1. Sign in to the ASAP web interface.
2. In the **Control panel** section, click **Import and synchronization**, and then open the **Open API** tab.
3. Click the **New token** button and select the API methods used for integration in the window that opens:
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid

4. Click the **Generate token** button.

5. Copy the token and save it in any convenient way. This token is required to configure integration in KUMA.

> The token is not stored in the ASAP system in the open form. After you close the **Get token** window, the token is unavailable for viewing. If you close the window without copying the token, you will need to click the **New token** button again for the system to generate a new token.

The issued token is valid for 12 months. After this period, the token is revoked. The issued token is also revoked if it is not used for 6 months.

Getting a link for API requests

To get the link used in ASAP for API requests:

1. Sign in to the ASAP web interface.

2. In the **Control panel** section, click **Import and synchronization**, and then open the **Open API** tab.

3. A link for accessing ASAP using the Open API is located at the bottom part of the window. Copy the link and save it in any convenient way. This link is required to configure integration in KUMA.

Configuring integration in KUMA

To configure KUMA integration with ASAP:

1. In the KUMA web interface, open **Settings** → **Integrations** → **Kaspersky Automated Security Awareness Platform** section.

   The **Kaspersky Automated Security Awareness Platform** window opens.

2. Make sure the **Status** toggle switch is enabled and the integration is enabled.

3. In the **Secret** drop-down list, select a secret to use for the Kaspersky Automated Security Awareness Platform integration. If necessary, you can also create a secret of the **token** type by specifying the token obtained in the ASAP platform. To do so:

   a. In the **Secret** drop-down list, click **Create**.

      This opens the **Create secret** window.

   b. In the **Name** field, enter the name of the secret. Must contain 1 to 128 Unicode characters.

   c. In the **Token** field, enter the authorization token for API requests to ASAP.

   d. If necessary, select the tags for the secret from the **Tags** drop-down list.

   e. If necessary, add the secret description in the **Description** field.

   f. Click **Create**.

4. In the **ASAP Open API URL** field, specify the address used by ASAP for API requests.

5. In the **ASAP administrator email** field, specify the email address of the ASAP administrator who receives notifications when users are added to the learning groups using KUMA.

6. In the **Notification template** drop-down list, select the template that you want KUMA to use for notifications. If necessary, you can also create a notification template by clicking **Create**.

7. If necessary, in the **Proxy** drop-down list select the proxy server resource to be used to connect to ASAP.

8. Click **Save**.

Integration with ASAP is configured in KUMA. When viewing information about alerts and incidents, you can select associated users to view which learning courses they have taken and to change their learning group.

Viewing information about the users from ASAP and changing learning groups

After configuring the integration between ASAP and KUMA, the following information from ASAP becomes available in alerts and incidents when you view data about associated users:

- The learning group to which the user belongs.
- The trainings passed by the user.
- The planned trainings and the current progress.
- The received certificates.

To view data about the user from ASAP:

1. In the KUMA web interface, in the **Alerts** or **Incidents** section, select the required alert or incident.

2. In the **Related users** section, click the desired account.

   The **Account details** window opens on the right side of the screen.

3. Select the **ASAP courses details** tab.

   The window displays information about the user from ASAP.

You can change the learning group of a user in ASAP.

To change a user learning group in ASAP:

1. In the KUMA web interface, in the **Alerts** or **Incidents** section, select the required alert or incident.

2. In the **Related users** section, click the desired account.

   The **Account details** window opens on the right side of the screen.

3. In the **Assign ASAP group** drop-down list, select the ASAP learning group you want to assign the user to.

4. Click **Apply**.

   The user is moved to the selected ASAP group, the ASAP company administrator is notified of the change in the learning group, and the study plan is recalculated for the selected learning group.

For details on learning groups and how to get started, refer to the ASAP documentation.

UserGate integration

This integration is an example and may require additional configuration depending on the versions used and the specifics of the infrastructure.
Compatibility is confirmed only for KUMA 2.0 or later and UserGate 6.0 or later.
The terms and conditions of premium technical support do not apply to this integration; support requests are processed without a guaranteed response time.

UserGate is a network infrastructure security solution that protects personal information from the risks of external intrusions, unauthorized access, viruses, and malware.

Integration with UserGate allows automatically blocking threats by IP address, URL, or domain name whenever KUMA response rules are triggered.

Configuring the integration involves the following steps:

1. Configuring integration in UserGate
2. Preparing a script for the response rule
3. Configuring the KUMA response rule

Configuring integration in UserGate

To configure integration in UserGate:

1. Connect to the UserGate web interface under an administrator account.

2. Go to **UserGate** → **Administrators** → **Administrator profiles**, and click **Add**.

3. In the **Profile settings** window, specify the profile name, for example, `API`.

4. On the **API Permissions** tab, add read and write permissions for the following objects:

   - content

   - core

- firewall
- nlists

5. Click **Save**.
6. In the **UserGate** → **Administrators** section, click **Add** → **Add local administrator**.
7. In the **Administrator properties** window, specify the login and password of the administrator.

   In the **Administrator profile** field, select the profile created at step 3.
8. Click **Save**.
9. In the address bar of your browser, after the address and port of UserGate, add `?features=zone-xml-rpc` and press **ENTER**.
10. Go to the **Network** → **Zones** section and for the zone of the interface that you want to use for API interaction, go to the **Access Control** tab and select the check box next to the **XML-RPC for management** service.

    If necessary, you can add the IP address of the KUMA correlator whose correlation rules must trigger blocking in UserGate, to the list of allowed addresses.
11. Click **Save**.

Preparing a script for integration with UserGate

To prepare a script for use:

1. Copy the ID of the correlator whose correlation rules you want to trigger blocking of URL, IP address, or domain name in UserGate:

   a. In the KUMA web interface, go to the **Resources** → **Active services**.

   b. Select the check box next to the correlator whose ID you want to obtain, and click **Copy ID**.

      The correlator ID is copied to the clipboard.
2. Download the script:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/
3. Open the script file and in the **Enter UserGate Parameters** section, in the **login** and **password** parameters, specify the credentials of the UserGate administrator account that was created at step 7 of configuring the integration in UserGate.
4. Place the downloaded script on the KUMA correlator server at the following path: /opt/kaspersky/kuma/correlator/<`correlator ID from step 1`>/scripts/.
5. Connect to the correlator server via SSH and go to the path from step 4:

   ```
   cd /opt/kaspersky/kuma/correlator/<correlator ID from step 1>/scripts/
   ```
6. Run the following command:

   ```
   chmod +x ug.py && chown kuma:kuma ug.py
   ```

The script is ready to use.

Configuring a response rule for integration with UserGate

To configure a response rule:

1. Create a response rule:

   a. In the web interface, select the **Resources** → **Response rules** section, and click **Add response rule**.

   b. This opens the **Create response rule** window; in that window, in the **Name** field, enter a name for the rule.

   c. In the **Tenant** drop-down list, select the tenant that owns the resource.

   d. In the **Type** drop-down list, select **Run script**.

   e. In the **Script name** field, enter the name of the script.

   ```
   ug.py.
   ```

   f. In the **Script arguments** field, specify the required operation and the KUMA field from which the value of the object to be blocked will be taken, depending on the operation:

   ```
   To block access by URL
   blockurl -i {{<KUMA field>}}
   ```

   ```
   To block access by IP address
   blockip -i {{<KUMA field>}}
   ```

   ```
   To block access by domain name
   blockdomain -i {{<KUMA field>}}
   ```

   ```
   Example
   blockurl -i {{.RequetstUrl}}
   ```

   g. In the **Conditions** section, add conditions corresponding to correlation rules that require blocking in UserGate when triggered.

   h. Click **Save**.

2. Add the response rule to the correlator:

   a. In the **Resources** → **Correlators** section, select the correlator that must respond and in whose directory you placed the script.

   b. In the steps tree, select **Response rules**.

   c. Then click the **Add** button.

   d. In the **Response rule** drop-down list, select the rule added at step 1 of these instructions.

e. In the steps tree, select **Setup validation**.

f. Click **Save and reload services**.

g. Click the **Save** button.

The response rule is linked to the correlator and ready to use.

Integration with Kaspersky Web Traffic Security

This integration is an example and may require additional configuration depending on the versions used and the specifics of the infrastructure.
Compatibility is confirmed only for KUMA 2.0 or later and Kaspersky Web Traffic Security 6.0 or later.
The terms and conditions of premium technical support do not apply to this integration; support requests are processed without a guaranteed response time.

You can configure integration with the Kaspersky Web Traffic Security web traffic analysis and filtering system (hereinafter also referred to as "KWTS").

Configuring the integration involves creating KUMA response rules that allow running KWTS tasks. Tasks must be created in advance in the KWTS web interface.

Configuring the integration involves the following steps:

1. Configuring integration in KWTS
2. Preparing a script for the response rule
3. Configuring the KUMA response rule

Configuring integration in KWTS

To prepare the integration in KWTS:

1. Connect to the KWTS web interface under an administrator account and create a role with permissions to view and create/edit a rule.

   For more details on creating a role, see the *Kaspersky Web Traffic Security Help*.

2. Assign the created role to a user with NTML authentication.

   You can use a local administrator account instead.

3. In the **Rules** section, go to the **Access** tab and click **Add rule**.

4. In the **Action** drop-down list, select **Block**.

5. In the **Traffic filtering** drop-down list, select the **URL** value, and in the field on the right, enter a nonexistent or known malicious address.

6. In the **Rule Name** field, enter the name of the rule.

7. Enable the rule using the **Status** toggle switch.

8. Then click the **Add** button.

9. In the KWTS web interface, open the rule you just created.

10. Make a note of the ID value that is displayed at the end of the page address in the browser address bar.

    You must use this value when configuring the response rule in KUMA.

The integration is prepared on the KWTS side.

Preparing a script for integration with KWTS

To prepare a script for use:

1. Copy the ID of the correlator whose correlation rules you want to trigger blocking of URL, IP address, or domain name in KWTS:

   a. In the KUMA web interface, go to the **Resources** → **Active services**.

   b. Select the check box next to the correlator whose ID you want to obtain, and click **Copy ID**.

      The correlator ID is copied to the clipboard.

2. To get the script and the library, please contact Technical Support.

3. Place the script provided by Technical Support on the KUMA correlator server at the following path: /opt/kaspersky/kuma/correlator/<`correlator ID from step 1`>/scripts/.

4. Connect to the correlator server via SSH and go to the path from step 3:

   ```
   cd /opt/kaspersky/kuma/correlator/< correlator ID from step 1 >/scripts/
   ```

5. Run the following command:

   ```
   chmod +x kwts.py kwtsWebApiV6.py && chown kuma:kuma kwts.py kwtsWebApiV6.py
   ```

The script is ready to use.

Configuring a response rule for integration with KWTS

To configure a response rule:

1. Create a response rule:

   a. In the web interface, select the **Resources** → **Response rules** section, and click **Add response rule**.

   b. This opens the **Create response rule** window; in that window, in the **Name** field, enter a name for the rule.

   c. In the **Tenant** drop-down list, select the tenant that owns the resource.

   d. In the **Type** drop-down list, select **Run script**.

   e. In the **Script name** field, enter the name of the script, kwts.py.

f. In the **Script arguments** field, specify the required operation and the KUMA field from which the value of the object to be blocked will be taken, depending on the operation:

```
To obtain a URL
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --url {{<KUMA field>}}
```

```
Example
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --url {{.RequestUrl}}
```

```
To obtain an IP address
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --ip {{<KUMA field>}}
```

```
Example
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --ip {{.DestinationAddress}}
```

```
To obtain a domain name
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --domain {{<KUMA field>}}
```

```
Example
```

```
--host <address> --username <user> --password <pass> --rule_id <id> --domain {{.DestinationHostName}}
```

Where:

- `--host` — address of the KWTS server.
- `--username` — name of the user account created in KWTS or local administrator.
- `--password` — KWTS user account password.
- `--rule_id`—ID of the rule created in KWTS.

If the KWTS user was created with NTLM authentication, add the key:

```
--ntlm
```

g. In the **Conditions** section, add conditions corresponding to correlation rules that require blocking in KWTS when triggered.

h. Click **Save**.

2. Add the response rule to the correlator:

a. In the **Resources** → **Correlators** section, select the correlator that must respond and in whose directory you placed the script.

b. In the steps tree, select **Response rules**.

c. Then click the **Add** button.

d. In the **Response rule** drop-down list, select the rule added at step 1 of these instructions.

e. In the steps tree, select **Setup validation**.

f. Click **Save and reload services**.

g. Click the **Save** button.

The response rule is linked to the correlator and ready to use.

Integration with Kaspersky Secure Mail Gateway

This integration is an example and may require additional configuration depending on the versions used and the specifics of the infrastructure.
Compatibility is confirmed only for KUMA 2.0 or later and Kaspersky Secure Mail Gateway 2.0 or later.
The terms and conditions of premium technical support do not apply to this integration; support requests are processed without a guaranteed response time.

You can configure integration with the Kaspersky Secure Mail Gateway mail traffic analysis and filtering system (hereinafter also referred to as "KSMG").

Configuring the integration involves creating KUMA response rules that allow running KSMG tasks. Tasks must be created in advance in the KSMG web interface.

Configuring the integration involves the following steps:

1. Configuring integration in KSMG
2. Preparing a script for the response rule
3. Configuring the KUMA response rule

Configuring integration in KSMG

To prepare the integration in KSMG:

1. Connect to the KSMG web interface under an administrator account and create a role with permissions to view and create/edit a rule.

   For more details on creating a role, see the *Kaspersky Secure Mail Gateway Help*.

2. Assign the created role to a user with NTML authentication.

   You can use the 'Administrator' local administrator account.

3. In the **Rules** section, click **Create**.

4. In the left pane, select the **General** section.

5. Enable the rule using the **Status** toggle switch.

6. In the **Rule Name** field, enter the name of the new rule.

7. Under **Mode**, select one of the message processing options that meets the criteria of this rule.

8. Under **Sender** on the **Email addresses** tab, enter a nonexistent or known malicious sender address.

9. Under **Recipient** on the **Email addresses** tab, specify the relevant recipients or the "*" character to select all recipients.

10. Click the **Save** button.

11. In the KSMG web interface, open the rule you just created.

12. Make a note of the ID value that is displayed at the end of the page address in the browser address bar.

    You must use this value when configuring the response rule in KUMA.

The integration is prepared on the KSMG side.

Preparing a script for integration with KSMG

To prepare a script for use:

1. Copy the ID of the correlator whose correlation rules must trigger the blocking of the IP address or email address of the message sender in KSMG:

   a. In the KUMA web interface, go to the **Resources** → **Active services**.

   b. Select the check box next to the correlator whose ID you want to obtain, and click **Copy ID**.

      The correlator ID is copied to the clipbord.

2. To get the script and the library, please contact Technical Support.

3. Place the script provided by Technical Support on the KUMA correlator server at the following path: `/opt/kaspersky/kuma/correlator/<correlator ID from step 1>/scripts/`.

4. Connect to the correlator server via SSH and go to the path from step 3:

```
cd /opt/kaspersky/kuma/correlator/<correlator ID from step 1>/scripts/
```

5. Run the following command:

```
chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py
```

The script is ready to use.

Configuring a response rule for integration with KSMG

To configure a response rule:

1. Create a response rule:

   a. In the web interface, select the **Resources** → **Response rules** section, and click **Add response rule**.

   b. This opens the **Create response rule** window; in that window, in the **Name** field, enter a name for the rule.

   c. In the **Tenant** drop-down list, select the tenant that owns the resource.

   d. In the **Type** drop-down list, select **Run script**.

   e. In the **Script name** field, enter the name of the script.

   ```
   ksmg.py
   ```

   f. In the **Script arguments** field, specify the required operation and the KUMA field from which the value of the object to be blocked will be taken, depending on the operation:

   ```
   To receive email
   --host <address> --username <user> --password <pass> --ntlm --rule_id <id> --email {{<KUMA field>}}
   ```

   ```
   Example
   --host <address> --username <user> --password <pass> --ntlm --rule_id <id> --email {{.SourceUserName}}
   ```

   ```
   To get an IP address
   --host <address> --username <user> --password <pass> --rule_id <id> --ip {{<KUMA field>}}
   ```

   ```
   Example
   --host <address> --username <user> --password <pass> --rule_id <id> --ip {{.SourceAddress}}
   ```

   Where:

   - `--host` — address of the KSMG server.
   - `--username` — name of the user account created in KSMG.
     You can specify the `Administrator` account.
   - `--password` — KSMG user account password.
   - `--rule_id`—ID of the rule created in KSMG.

   If the KWTS user was created with NTLM authentication, add the following key:

   ```
   --ntlm
   ```

g. In the **Conditions** section, add conditions corresponding to the correlation rules that when triggered require blocking the IP address or email address of the message sender in KSMG.

h. Click **Save**.

2. Add the response rule to the correlator:

a. In the **Resources** → **Correlators** section, select the correlator that must respond and in whose directory you placed the script.

b. In the steps tree, select **Response rules**.

c. Then click the **Add** button.

d. In the **Response rule** drop-down list, select the rule added at step 1 of these instructions.

e. In the steps tree, select **Setup validation**.

f. Click **Save and reload services**.

g. Click the **Save** button.

The response rule is linked to the correlator and ready to use.

Kaspersky Managed Detection and Response integration

Kaspersky Managed Detection and Response (hereinafter also MDR) is a solution for automatic detection and analysis of security incidents in your infrastructure using telemetry and advanced machine learning technologies.

You can configure the Kaspersky Managed Detection and Response integration in KUMA to automatically import incidents from the MDR Console into KUMA for further processing and analysis.

To configure the integration:

1. Perform the preliminary configuration.

2. Configure the MDR integration.

Preliminary configuration

To perform preliminary configuration for MDR integration:

1. Provide access to the MDR Console.

   Make sure that the KUMA server on which you want to configure integration has network access to https://mdr.kaspersky.com on port **TCP/443**

2. In KUMA, create a user with the Junior analyst role.

Make sure this user has access to the API and can make the following requests:

- `POST /events`
- `POST /incidents/create`
- `POST /incidents/comment`
- `POST /incidents/close`

3. In the MDR Console, generate an API token by following these steps:

   a. In the MDR Console window, select the **Settings** menu item.

   b. Select the **API** tab.

   c. In the upper part of the window, click the **Add** button.

   d. Specify a **Connection name**. This name will be displayed as the user name when incidents, comments, and attachments are created because the access token is not tied to a specific user.

   The connection name can contain Latin letters, numerals, and special characters.

   e. In the **User role** drop-down list, select the **MDR Administrator** role.

   f. In the **Tenant** drop-down list, select the tenant whose incidents you want to import into KUMA.

   Select one or more tenants, if necessary.

   > If there is no value in the **Tenant** drop-down list for incidents created in the MDR Console, specify **Root tenant** to let the script discover such incidents when connecting.

   g. Then click the **Create** button.

   The solution displays the values of the following settings:

   - **JWT token** (`refresh token`) is the primary token that is used to get the `refresh token / access token` pair.
   - **ClientID** (`client id`) is the client ID that must be sent when making requests to the MDR API.

   > Save these values because they will be required at the integration initialization stage.

4. Download the contents of the MDR-integrations repository from GitHub.

   To get this data, you can also clone the repository directly to the KUMA server by running the following command:

```
git clone https://github.com/klsecservices/MDR-integrations.git
```

5. Download the certificate chain for MDR in PEM format by following these steps:

   a. In your browser, open the https://mdr.kaspersky.com link.

   b. Click the padlock icon in the address bar next to the URL of the website.

   c. Select **Connection is secure** and click **Certificate is valid**.

   d. Select the **Details** tab.

   e. For each item in the certificate hierarchy (starting with the lowest, ***.mdr.kaspersky.com**, and ending with the root, **DigiCert Global Root G2**), click the **Export** button.

   f. Add the saved certificates to a .PEM file (`mdr.pem`) by running the following command:

```
cat "DigiCert Global G2 TLS RSA SHA256 2020 CA1.crt" "DigiCert Global Root G2.crt" "_.mdr.kaspersky.crt" >
mdr.pem
```

   > You will need the `mdr.pem` file thus obtained at the integration initialization step.

Initializing integration

To configure KUMA integration with Kaspersky Managed Detection and Response:

1. Set up the configuration file by following these steps:

   a. Go to the `./conf` directory and open the `config.yml` file for editing (you can start by copying the sample_config.yml file).

   b. In the `General settings` section, specify the client ID (the `client_id` setting).

   c. In the `Modules settings` → `kuma` section, specify the following settings:

   - `api_url` is the address of the KUMA API.
   - `api_token` is the token for access to the KUMA API.
   - `tenantId` is ID of the tenant to which incidents will be imported.

   You can also manage other integration settings. To do this, read the comments to the settings in the sample_config.yml file.

2. Add an MDR authorization token by following these steps:

   a. Go to the `./conf` directory and open the `.refresh_token` file for editing.

   b. Paste the previously generated MDR API access token into the file.

3. Specify when to start collecting incidents:

   a. Go to the `./conf` directory and open the `.last_check` file for editing.

   b. In this file, specify the timestamp (in milliseconds, 13 digits) from which you want to import incidents.

      To check whether the configuration is correct, we recommend specifying a time before the last incident occurred (for example, `1672520400000`).

4. Update the MDR certificate. In the `./conf/` directory, replace the `mdr.pem` file with a file containing the up-to-date certificate that you created earlier.

5. Run the `main.py` integration script using the following command:

   ```
   python3 ./main.py
   ```

   If you see messages about missing required packages when you start the script for the first time, install these packages.

   If no error messages are displayed after running the script (except for warnings about an invalid certificate), the integration is configured correctly.

   You can find the script log in the `./log/app.log` directory.

6. Check the import of incidents.

   Make sure that incidents created in the MDR Console, starting from the time that you specified in the `.last_check` file, have been imported into KUMA.

7. Run the script in the background by following these steps:

   a. Stop the currently running script (if running).

   b. Run the `main.py` script again in the background with the following command:

      ```
      nohup python3 /opt/mdr/main.py &
      ```

8. Configure the script to run automatically after a server restart:

   ```
   sudo crontab -e
   @reboot sleep 300 && python3 /opt/mdr/main.py &
   ```

   A delay of 5 minutes (`sleep 300`) is necessary to start the kuma-core service before starting the integration script.

Integration of KUMA with Kaspersky Managed Detection and Response is now configured. From now on, incidents from the MDR Console will be automatically imported into KUMA for processing and analysis.

Importing asset information from RedCheck

This integration is an example and may require additional configuration depending on the versions used and the specifics of the infrastructure.
Compatibility is confirmed only for KUMA 2.0 or later and RedCheck 2.6.8 or later.
The terms and conditions of premium technical support do not apply to this integration; support requests are processed without a guaranteed response time.

RedCheck is a system for monitoring and managing the information security of an organization. You can import asset information into KUMA from reports of network device scans performed with RedCheck. Import is available from simple "Vulnerabilities" and "Inventory" reports in CSV format, grouped by hosts.

Data is imported through the API using the redcheck-tool.py utility. The utility requires Python 3.6 or later and the following libraries:

- csv
- re
- json
- requests
- argparse
- sys

Imported assets are displayed in the KUMA web interface in the **Assets** section. If necessary, you can edit the settings of assets.

To import asset information from a RedCheck report:

1. Generate a network asset scan report in RedCheck in CSV format and copy the report file to the server where the script is located.

   For more details about scan tasks and output file formats, refer to the RedCheck documentation.

2. Create a file with the token for accessing the KUMA REST API.

   The account for which the token is created must satisfy the following requirements:

   - Tenant administrator or Tier 2 analyst role.
   - Access to the tenant into which the assets will be imported.
   - Rights to use API requests: GET /assets, GET /tenants, POST/assets/import.

3. Download the script via the following link:

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

4. Copy the `redcheck-tool.py` utility to the server hosting the KUMA Core, and make the tool's file executable using this command:

```
chmod +x <path to the redcheck-tool.py file>
```

5. Run the `redcheck-tool.py` utility using the following command:

```
python3 redcheck-tool.py --kuma-rest <address and port of the KUMA REST API server> --token <API token> --
tenant <name of the tenant in which the assets must be placed> --vuln-report <full path to the
"Vulnerabilities" report file> --inventory-report <full path to the "Inventory" report file>
```

Example

```
python3 --kuma-rest kuma.example.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report
/home/user/vuln.csv --inventory-report /home/user/inventory.csv
```

You can use additional flags and commands for import operations. For example, the command displaying an extended report on the received assets

```
-v
```

See available flags and commands of redcheck-tool.py

Flags and commands	Mandatory	Description
`--kuma-rest <address and port of the KUMA server>`	Yes	Port 7223 is used for API requests by default. You can change the port if necessary.
`--token <token>`	Yes	The value of the option must contain only the token. The Tenant administrator or Tier 2 analyst role must be assigned to the user account for which the API token is being generated.
`--tenant <tenant name>`	Yes	Name of the KUMA tenant to which you want to import assets from the RedCheck report.
`--vuln-report <full path to the "Vulnerabilities" report>`	Yes	"Vulnerabilities" report file in CSV format.
`--inventory-report <full path to the "Inventory" report file>`	No	"Inventory" report file in CSV format.
`-v`	No	Display extended information about the import of assets.

To view information about available flags and commands, run the following command:

```
--help
```

The asset information is imported from the RedCheck report to KUMA. The console displays information on the number of new and updated assets.

Example

```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

Example of extended import information

```
[inventory import]          Host: localhost        Code: 200  Response: {'insertedIDs': {'0': '52ca11c6-a0e6-
4dfd-8ef9-bf58189340f8'}, 'updatedCount': 0, 'errors': []}
```

```
[inventory import]          Host: 10.0.0.2         Code: 200  Response: {'insertedIDs': {'0': '1583e552-5137-
4164-92e0-01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error]    Host: localhost        Skipped asset with FQDN localhost or IP 127.0.0.1
[software import]           Host: 10.0.0.2         Code: 200  Response: {'insertedIDs': {}, 'updatedCount': 1,
'errors': []}
[vulnerabilities import]    Host: 10.0.0.2         Code: 200  Response: {'insertedIDs': {}, 'updatedCount': 1,
'errors': []}
[vulnerabilities import]    Host: 10.0.0.1         Code: 200  Response: {'insertedIDs': {'0': '0628f683-c20c-
4107-abf3-d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import]    Host: localhost        Code: 200  Response: {'insertedIDs': {}, 'updatedCount': 1,
'errors': []}
[vulnerabilities import]    Host: 10.0.0.3         Code: 200  Response: {'insertedIDs': {'0': 'ed01e0a8-dcb0-
4609-ab2b-91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)
```

The utility works as follows when importing assets:

- KUMA overwrites the data of assets imported through the API, and deletes information about resolved vulnerabilities.
- KUMA skips assets with invalid data.

The table below lists errors that may occur when importing asset information from RedCheck.

Possible errors

Error message	Description
Tenant %w not found	The tenant name was not found.
Tenant search error: Unexpected status Code: %d	An unexpected HTTP response code was received while searching for the tenant.
Asset search error: Unexpected status Code: %d	An unexpected HTTP response code was received while searching for an asset.
[%w import][error] Host: %w Skipped asset with FQDNlocalhost or IP 127.0.0.1	When importing inventory/vulnerabilities information, host with fqdn=localhost or ip=127.0.0.1 was skipped.

Storing events

KUMA storage is a service designed to store normalized events and provide fast access to them for analytical data extraction. The storage is a ClickHouse cluster associated with the storage service and other KUMA services. The storage service receives data from collectors and correlators, transfers it to ClickHouse, and allows you to configure data storage settings.

Built-in ClickHouse mechanisms provide database clustering, data transfer between hot and cold storage, and data archiving. ClickHouse clusters can be supplemented with cold storage disks.

Normalized events are stored on network infrastructure servers where a cluster of ClickHouse nodes is deployed.

Before creating storage, the required network infrastructure must be deployed, taking into account your organization's requirements for event storage. For more information, please refer to the ClickHouse documentation.

In storage, you can create *spaces* to organize the data structure, for example, to store events of a certain type together.

Recommendations for storage servers

You need to use high-speed protocols, such as Fibre Channel or iSCSI 10G, to connect the data storage system to storage servers. We do not recommend using application-level protocols, such as NFS or SMB for that purpose.

It is recommended to use ext4 as the file system on ClickHouse cluster servers.

When using RAID arrays, it is recommended:

- to ensure high performance: RAID 0;
- to ensure high performance and high availability: RAID 10.

To ensure high availability and performance of your data storage subsystem, we recommend deploying ClickHouse nodes on different disk arrays.

When using a virtual infrastructure, it is recommended to deploy ClickHouse cluster nodes on different hypervisors. In this case, it is required to ensure that two ClickHouse virtual machines are not placed on the same hypervisor.

For highly loaded Kaspersky SIEM instances, it is recommended to use hardware servers to host ClickHouse.

Recommendations for using system memory

If you are creating storage on systems with limited memory and want to limit memory consumption, it is recommended that you determine the amount of memory used and increase the value of the `max_server_memory_usage` parameter. This setting determines the maximum amount of memory that the server can use. This value is specified in bytes.

By default, `max_server_memory_usage` is assigned `0` value. In this case, the server can use all the available memory.

The value of the `max_server_memory_usage` parameter is also limited by the `max_server_memory_usage_to_ram_ratio` parameter, which defines the ratio of used memory to total available memory. For example, a value of 0.9 means that the server can use up to 90% of the available memory.

When determining current memory usage, keep in mind the following limitations:

- The optimal amount of memory available to storage is about 75% of the total system memory.

  > It is not recommended to use 100% of the available memory, as this may result in insufficient memory for processing incoming requests.

- If other applications are installed on the server, you need to allocate enough memory for their operation.
- If you change the hardware configuration of the server on which the storage is deployed, adjust the memory usage settings accordingly.

About the ClickHouse cluster

A ClickHouse cluster is a logical group of devices that includes shards, replicas, and keepers, which together provide storage of all normalized Kaspersky SIEM events, their replication, and coordination of cluster operations. A cluster can include one or more *shards*.

A *shard* is a logical group of devices containing a **portion** of all normalized events accumulated in the cluster. Increasing the number of shards lets you do the following:

- Accumulate more events by increasing the total number of servers and disk space.
- Process a larger event stream by balancing the load when recording new events.
- Reduce the time taken to search for events by distributing search zones among multiple devices.

A shard can include one or more *replicas*.

A *replica* is a device that is part of a shard and contains a copy of its data. If multiple replicas exist, there would be multiple copies (the data gets replicated). Increasing the number of replicas lets you do the following:

- Increase fault tolerance.
- Distribute the load associated with data retrieval across multiple devices.

A *keeper* is a device that participates in coordination of data replication at the entire cluster level. A cluster requires at least one keeper. The number of keepers must be odd. It is recommended to use three devices with the Keeper role. The keeper and replica roles can be combined.

Before creating ClickHouse cluster nodes, make sure there is network connectivity among system components and open the necessary network ports.

Creating a storage

Storage creation is comprised of the following stages:

1 Creating a resource set for a storage in the Kaspersky SIEM web interface

A storage service is created based on the set of resources for the storage.

1. Under **Resources** → **Storage**, click **New**.

   This opens the **Create storage** window.

2. On the **Basic settings** tab, in the **Storage name** field, enter a unique name for the service you are creating. The name must contain 1 to 128 Unicode characters.

3. In the **Tenant** drop-down list, select the tenant that will own the storage.

4. In the **Tags** drop-down list, select the tags for the resource set that you are creating.

   The list includes all available tags created in the tenant of the resource and in the Shared tenant. You can find a tag in the list by typing its name in the field. If the tag you entered does not exist, you can press **`Enter`** or click **Add** to create it.

5. Add a description for the service in the **Description** field. It must contain 1 to 256 Unicode characters.

6. In the **Retention policy options** field, select an event storage condition in the ClickHouse cluster for the storage, which, when satisfied, will cause events to be transferred to cold storage disks or deleted if cold storage is not configured or is configured incorrectly, starting from partitions for the oldest date.

   The condition is applied to the default space and to events from deleted spaces.

   By default, ClickHouse moves events to cold storage disks or deletes them if more than 97% of the storage is full. KUMA also applies an additional **365 days** storage condition when creating a storage.

   To set the storage condition, do one of the following:

   - If you want to limit the storage period for events, select **Days** from the drop-down list, and in the field, specify the maximum event storage period (in days) in the ClickHouse hot storage cluster.

     The minimum value is 1. The default value is 365.

   - If you want to limit the maximum storage size, select **GB** from the drop-down list, and in the field, specify the maximum storage size in gigabytes.

     The minimum and default value is 1.

   - If you want to limit the storage size to a percentage of disk space that is available to the storage, select **Percent** from the drop-down list and specify the maximum storage size as a percentage of the available disk space.

     You can get information about available disk space in ClickHouse by running the query:

     ```
     'SELECT hostname(), name, total_space FROM system.disks'
     ```

     Possible values: 1 to 95. The default value is 80. If you want to use percentages for all storage spaces, the sum total of percentages in the conditions of all spaces may not exceed 95, but we recommend specifying a limit of at most 90% for the entire storage or for individual spaces.

     We do not recommend specifying a value less than 5% as this increases the likelihood of data loss in the storage.

     > If the storage is organized as a cluster, the amount of occupied disk space is determined for each of the several servers separately. Stored data may be unevenly distributed among disks on the servers. KUMA shifts events to cold storage disks or deletes them when the maximum storage size is reached *on any individual server in the cluster*.

The algorithm for determining the size of occupied storage space

The size of occupied storage space is determined as follows:

1. Information about the state of KUMA disks and partitions is obtained from all available replicas.

2. If occupied space exceeds the configured values, KUMA takes action depending on the type of data storage: hot or cold.

For hot storage, the following actions are performed for each available node and space:

a. The total size of the partitions of this space on the replica is calculated.

b. The maximum space size on the replica is calculated:

- If an absolute value in GB is set for the storage size, the maximum space size on the replica is calculated as follows:

  ```
  <maximum space size> = <configured threshold> / <number of replicas in the cluster>
  ```

  For example, consider a cluster with three shards, each of which contains two replicas; a threshold of 6 GB is set, and the maximum size of data on a replica is 1 GB.

- If a relative value is set for the storage size as a percentage, the maximum space on the replica is calculated as follows:

  ```
  <maximum space size> = <space size on the replica> / <size of the replica disk> * 100%
  ```

  > The size of the replica disk does not include the space reserved for `ext4`.

If the specified threshold is exceeded, partitions on the host are deleted or moved to cold storage. Partitions are deleted on all shards.

For cold storage, partitions are deleted for each available space in accordance with the event retention period (TTL) configured in KUMA.

If you want to use an additional storage condition, click **Add policy options** and specify an additional storage condition. The maximum number of conditions is two, and you can combine only conditions the following types:

- Days and storage size in GB
- Days and storage size as a percentage

If you want to remove a storage condition, click the X icon next to this condition.

7. In the **Audit retention period** field, specify the period, in days, to store audit events. The minimum value and default value is `365`.

8. If you want to change ClickHouse settings, in the **ClickHouse configuration override** field, paste the lines with settings from the ClickHouse configuration XML file `/opt/kaspersky/kuma/clickhouse/cfg/config.xml`.

   When specifying the `<yandex>` root elements, `</yandex>` is not required. Settings passed in this field are used instead of the default settings.

   Example

   ```
   <merge_tree>
   <parts_to_delay_insert>600</parts_to_delay_insert>
   <parts_to_throw_insert>1100</parts_to_throw_insert>
   </merge_tree>.
   ```

9. If necessary, in the **ClickHouse cluster nodes** section, add ClickHouse cluster nodes to the storage.

   There can be multiple nodes. You can add nodes by clicking the **Add node** button or remove nodes by clicking the X icon of the relevant node.

Specify the following settings:

- In the **FQDN** field, enter the fully qualified domain name of the node that you want to add. For example, `kuma-storage-cluster1-server1.example.com`.

- In the **Shard ID**, **Replica ID**, and **Keeper ID** fields, specify the role of the node in the ClickHouse cluster.

  The shard and keeper IDs must be unique within the cluster. The replica ID must be unique within the shard.

  The combination of identifiers determines the position of the node in the structure of the cluster and its functional purpose:

  - Shard, replica, keeper: the node participates in the accumulation and search of normalized events, and helps coordinate data replication at the cluster-wide level.

  - Shard, replica: the node participates in the accumulation and search of normalized events.

  - Keeper: the node does not store normalized events, but helps coordinate data replication at the cluster-wide level.

    It is recommended to specify dedicated nodes with the keeper role at the beginning of the list in the **Resources** → **Storages** → **<Storage>** → **Basic settings** → **ClickHouse cluster nodes** section.

The following example shows how to populate the **ClickHouse cluster nodes** section for a storage with dedicated keepers in a distributed installation. You can adapt this example according to your needs.

Example: ClickHouse cluster nodes

```
        FQDN: kuma-storage-cluster1-server1.example.com
                Shard ID: 0
        Replica ID: 0
        Keeper ID: 1
                FQDN: kuma-storage-cluster1server2.example.com
                Shard ID: 0
        Replica ID: 0
        Keeper ID: 2
                FQDN: kuma-storage-cluster1server3.example.com
                Shard ID: 0
        Replica ID: 0
        Keeper ID: 3
                FQDN: kuma-storage-cluster1server4.example.com
                Shard ID: 1
        Replica ID: 1
        Keeper ID: 0
                FQDN: kuma-storage-cluster1server5.example.com
                Shard ID: 1
        Replica ID: 2
        Keeper ID: 0
        FQDN: kuma-storage-cluster1server6.example.com
                Shard ID: 2
        Replica ID: 1
        Keeper ID: 0
                FQDN: kuma-storage-cluster1server7.example.com
                Shard ID: 2
        Replica ID: 2
        Keeper ID: 0
```

10. To distribute stored objects across spaces, create them in the **Spaces** settings section.

    How to create a space in the storage

    There can be multiple spaces. You can add spaces by clicking the **Add space** button or remove spaces by clicking the X icon of the relevant space.

Specify the following settings:

1. In the **Name** field, specify a name for the space containing 1 to 128 Unicode characters.

2. To prevent a space from receiving events, select the **Read only** check box.

   This check box is cleared by default.

3. In the **Retention policy options** field, select an event storage condition in the ClickHouse cluster for the space, which, when satisfied, will cause events to be transferred to cold storage disks or deleted if cold storage is not configured or is configured incorrectly. KUMA applies the **365 days** storage condition when a space is added.

   To set the storage condition for a space, do one of the following:

   - If you want to limit the storage period for events, select **Days** from the drop-down list, and in the field, specify the maximum event storage period (in days) in the ClickHouse hot storage cluster.

     The minimum value is 1. The default value is 365.

   - If you want to limit the maximum storage space size, select **GB** from the drop-down list, and in the field, specify the maximum space size in gigabytes.

     The minimum value and default value is 1.

   - If you want to limit the space size to a percentage of disk space that is available to the storage, select **Percent** from the drop-down list, and in the field, specify the maximum space size as a percentage of the size of the disk available to the storage. In this case, the condition can also be triggered when the disk space available to the storage is decreased.

     Possible values: 1 to 95. The default value is 80. If you want to use percentages for all storage spaces, the sum total of percentages in the conditions of all spaces may not exceed 95, but we recommend specifying a limit of at most 90% for the entire storage or for individual spaces.

     We do not recommend specifying small percentage values as this increases the probability of data loss in the storage.

     > When using size as the storage condition, you must ensure that the total size of all spaces specified in the storage conditions does not exceed the physical size of the storage, otherwise an error will be displayed when starting the service.

     > In storage conditions with a size limitation, use the same units of measure for all spaces of a storage (only gigabytes or only percentage values). Otherwise, if the condition is specified as a percentage for one space, and in gigabytes for another space, the storage may overflow due to mismatch of values, leading to data loss.

4. If necessary, in the **Event retention time** field, specify the total KUMA event storage duration in days, counting from the moment when the event is received. When the specified period expires, events are automatically deleted from the cold storage disk. The default value is 0.

   The **Event retention time** setting becomes available only after adding at least one cold storage disk.

   The event retention time is calculated as the sum of the event retention time in the ClickHouse hot storage cluster until the condition specified in the **Retention policy options** setting is triggered, and the event retention time on the cold storage disk. After one of storage conditions is triggered, the data partition for the earliest date is moved to the cold storage disk, and there it remains until the event retention time in KUMA expires.

Depending on the specified storage condition, the resulting retention time is as follows:

- If you specify a storage condition in days and want events to be moved to cold storage, the value of the **Event retention time** setting must be greater than the number of days defined in the storage condition. The cold storage duration for events is calculated as the **Event storage time** minus the number of days specified in the **Retention policy options** setting.

  If you do not want to store events from this space on the cold storage disk, you can specify the same number of days in the **Event retention time** field as in the storage condition.

- If you specify a storage condition in gigabytes or percentages and want events to be moved to cold storage, it is recommended to set a relatively large value for the **Event retention time** setting to avoid deleting events. This is because it is impossible to calculate the exact date when the conditions specified in the **Retention policy options** will be met.

  If you do not want to store events from this space on the cold storage disk, you can set **Event retention time** to 0.

5. To define which events are moved into a space, in the **Filter settings** section, select a ready-made filter from the **Filter** drop-down list or create a new one by clicking the **New** button.

   Creating a filter in resources

   All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

   To create a filter:

   1. In the **Filter** drop-down list, select **Create new**.

   2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

   3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

   4. Select the filter creation mode: **Constructor** or **Code**.

      When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

   5. If you selected the **Constructor** option, do the following:

      a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

      b. Click the **Add condition** button.

      c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

d. From the drop-down lists, select operands and filter operators.

Operands of filters

- **Event fields** specify the field of the event that you need to use as a filter operand.
- **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

  If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
- **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the dictionary that you want to use.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
  - **context table name** (required) is the context table that you want to use.
  - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
  - **field** is the name of the context table field from which you want to get the value of the operand.
  - **index** is the index of the list field of the table from which you want to get the value of the operand.
- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.

- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.

- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.

- **inContextTable** checks for the presence of the entry in the specified context table.

- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ×.

8. Click **Save**.

Once the space is created, you can view and delete spaces in the storage resource set settings.

> There is no need to create a separate space for audit events. Events of this type (Type=4) are automatically placed in a separate Audit space with a storage term of at least 365 days. This space cannot be edited or deleted from the KUMA web interface.

11. To transfer events for long-term storage from the ClickHouse cluster to disks, add disks to storage in the **Disks for cold storage** section.

12. **How to add a disk to storage**

    There can be multiple disks. You can add disks by clicking the **Add disk** button, or remove them by clicking the X icon in a corresponding disk's block.

    Specify the following settings:

    1. In the **Type** drop-down list, select the type of the domain name of the disk being connected:

       - **Local**—for the disks mounted in the operating system as directories.

       - **HDFS**—for the disks of the Hadoop Distributed File System.

- **S3**—for S3 cloud storage disks used in KUMA.

  > Starting with version 4.2, data stored on HDFS drives will be gradually migrated to S3 storage disks. Support for the HDFS file system will be discontinued in one of future releases of KUMA.

2. In the **Name** field, specify the disk name.

   Rules for naming an S3 storage

   When assigning a name to an S3 storage, the following requirements must be met:

   - The name must be unique within a single storage.
   - The name may include lowercase Latin letters and numerals. You can also use the underscore character (_) in the name.

     Non-Latin letters are not allowed.
   - The name must contain 1 to 128 Unicode characters.

   > You cannot change the name of an S3 storage disk without changing the path to the disk.

3. Depending on the selected type, do one of the following:

   - If you select the **Local** domain name type for the disk, specify the absolute directory path of the mounted local disk in the **Path** field. The path must begin and end with a "/" character.

     The directory of the mounted local disk must be owned by the KUMA user.
   - If you select **HDFS** domain name type for the disk, specify the path to HDFS in the **Host** field. For example, `hdfs://hdfs1:9000/clickhouse/`.
   - If you selected **S3** as the domain name type for the disk, perform the following actions:

     a. In the **Host** field, enter the address of the S3 storage (for example, `https://www.company.com/clickhouse/storagefolder/`).

     Rules for specifying the address of the S3 storage

     When specifying an S3 storage address, the following requirements must be satisfied:

     - The address must be specified in the URL format, for example:

       `https://<web address/IP address of the server>/<path to disk>/`
     - The address must end with a "/" character.
     - The maximum length is 2048 characters.
     - Non-Latin letters are not allowed.

     > You cannot change the address of an S3 storage disk without changing the name of the disk.

     b. In the **Secret** field, specify the secret for access to the S3 storage. You can select a secret from the drop-down list or create a secret by clicking **Create new**.

c. In the **Certificate chain** field, specify the path to the file with the complete certificate trust chain for connecting to the S3 storage.

   You must fill in this field if you are connecting to the S3 storage via HTTPS. If you are using HTTP, you do not need to specify a certificate. The file must contain the full BASE64-encoded certificate trust chain, including the root certificate, intermediate (if any), and S3 storage certificate.

4. Return to the basic settings section and fill in the following fields:

   - **Event retention time** specifies the total KUMA event storage duration in days, counting from the moment when the event is received. When the specified period expires, events are automatically deleted from the cold storage disk. The default value is 0.

     The event retention time is calculated as the sum of the event retention time in the ClickHouse hot storage cluster until the condition specified in the **Retention policy options** setting is triggered, and the event retention time on the cold storage disk. After one of storage conditions is triggered, the data partition for the earliest date is moved to the cold storage disk, and there it remains until the event retention time in KUMA expires.

     Depending on the specified storage condition, the resulting retention time is as follows:

     - If you specify a storage condition in days and want events to be moved to cold storage, the value of the **Event retention time** setting must be greater than the number of days defined in the storage condition. The cold storage duration for events is calculated as the **Event storage time** minus the number of days specified in the **Retention policy options** setting.

       If you do not want to store events from this space on the cold storage disk, you can specify the same number of days in the **Event retention time** field as in the storage condition.

     - If you specify a storage condition in gigabytes or percentages and want events to be moved to cold storage, it is recommended to set a relatively large value for the **Event retention time** setting to avoid deleting events. This is because it is impossible to calculate the exact date when the conditions specified in the **Retention policy options** will be met.

       If you do not want to store events from this space on the cold storage disk, you can set **Event retention time** to 0.

   - **Audit cold retention period**—the number of days to store audit events. The minimum value is 0.

13. To configure backup and restore for the storage, set the required settings.

    How to configure backup and restore

    Configure the following settings:

    1. In the **Storage backup** field, specify the path for storing the backup file, for example `/mnt/data`, taking into account the following requirements:

       - The path must be the same on all nodes of the storage cluster.

       - The path must not contain prefixes.

         List of prefixes that cannot be added to file paths

         Prefixes that cannot be used when specifying paths to files:

         - `/*`

         - `/bin`

         - `/boot`

- `/dev`
- `/etc`
- `/home`
- `/lib`
- `/lib64`
- `/proc`
- `/root`
- `/run`
- `/sys`
- `/tmp`
- `/usr/*`
- `/usr/bin/`
- `/usr/local/*`
- `/usr/local/sbin/`
- `/usr/local/bin/`
- `/usr/sbin/`
- `/usr/lib/`
- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path.

Files are available at the following paths:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

- The user must have read, write, and execute permissions in the specified directory.
- The specified directory must belong to the second or deeper nesting level. Using a directory at the first nesting level, for example `/backup` is not allowed.
- The directory name may not contain a period.

Two directories are automatically created at the specified path: **backup** and **restore**. If no path is specified, the scheduled backup, manual backup, restoration from backup, and import functions are not available.

2. To configure scheduled backup, select the **Add automatic backup** check box and do the following:

   a. In the **Back up after several days** field, enter an integer to specify how many days after a partition is created you want a backup copy of it to be created. For example, if the value is **1**, backup is performed for the partition created the day before yesterday.

   b. In the **Replicas** drop-down list, select one replica that you want to back up. Selecting multiple replicas of the same shard causes data duplication.

   c. Under **Partitions**, click **Add partition** and set the following settings:

      - In the **Tenant** drop-down list, select the tenant that contains the partition that you want to back up.
      - In the **Spaces** drop-down list, select one or more storage spaces that belong to the partition that you want to back up. If no value is specified, the whole partition is backed up.

      You can add multiple partitions. For example, if you want to back up the **Audit** space and you have 10 tenants, you must configure the backup separately for each tenant.

14. If necessary, go to the **Advanced settings** tab and configure the following settings:

- In the **Buffer size** field, enter the buffer size in bytes that, when reached, will trigger sending the events to the database. The default value is 128 MB. If the virtual computer has less free RAM than the specified **Buffer size**, 128 MB limit will be set.

  If the expected traffic to the storage service is greater than 1 Gbps, we recommend changing the **Buffer size** setting to the expected value and setting the **Buffer flush interval** to 2.

  The value of the **Buffer size** setting can be determined empirically. If the **Insert QPS** metric of the storage is greater than 1 and the queue of requests is building up, follow the recommendations for calculating and adjusting the **Buffer size** setting provided in the Viewing KUMA metrics article.

- In the **Maximum buffer size** field, specify the maximum buffer size in bytes. The default value is 256 MB.

  By default, events are written to the database once per second. If the EPS rises and events are registered more often than once per second, the buffer size is automatically increased. The buffer is increased up to three times the **Buffer size** value, but cannot exceed the **Maximum buffer size** value. When the load goes back to normal, the buffer size stays the same; there is no automatic reduction of buffer size.

  If the **Maximum buffer size** is less than or equal to the **Buffer size**, the buffer size does not change.

  Restarting the storage service resets the increased buffer size to the value in the **Buffer size** field.

- In the **Buffer flush interval** field, enter the time in seconds for the solution to wait for the buffer to fill up. If the buffer is not full and the specified time has elapsed, events are sent to the database. The default value is 1 second.

- In the **Required memory size** field, specify the minimum amount of free RAM in bytes. The default value is 0.

  If the node on which the storage is installed has less free RAM than this setting, database insert request returns an error, and the events are recorded later. Limiting the memory size allows avoiding the situation when the memory fills up if, for any reason, the recording of events in the database is blocked and data begins to accumulate in memory.

- In the **Disk buffer size limit** field, enter a value in bytes.

  The disk buffer is used to temporarily store events that could not be sent for further processing or storage. If the disk space allocated for the disk buffer is exhausted, events are rotated as follows: new events replace the oldest events written to the buffer. The default value is 10 GB.

- Use the **Disk buffer** toggle switch to enable or disable the disk buffer. By default, the disk buffer is enabled.

- Use the **Write to local database table** toggle switch to enable or disable writing to the local database table. Writing is disabled by default.

  If enabled, data is written only on the host on which the storage is located. We recommend using this functionality only if you have configured balancing on the collector and/or correlator at step **6. Routing**, in the **Advanced settings** section, the **URL selection policy** field is set to **Round robin**.

  If you disable writing, the data is distributed across the shards of the cluster.

- Use the **Debug** toggle switch to enable logging of service operations.

- You can use the **Create dump periodically** toggle switch at the request of Technical Support to generate resource utilization reports (e.g., CPU or RAM) as dumps.

- In the **Dump settings** field, you can specify the settings to be used when creating dumps. For instructions on filling out this field, please contact Technical Support.

The set of resources for the storage is created and is displayed under **Resources** → **Storages**.

2 Creating a storage service

After creating the storage resource set, create a storage service:

1. Under **Resources** → **Active services**, click **Add service**.

2. In the **Choose a service** window that opens, select the resource set that you created for the storage, and click **Create service**.

The storage service is created and is displayed under **Resources** → **Active services**. Now the storage service must be installed on each node of the ClickHouse cluster by using the service ID. To do this, in the **Resources** → **Active services** section, in the context menu of the created storage service, click **Copy ID**.

3 Installing a storage service in a network infrastructure

When installing the storage service on cluster nodes, ensure network connectivity and open the ports used by the components.

1. Log in to the server where you want to install the storage service.

2. Install the storage service using the command:

```
sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --install
```

   where:

   - <FQDN> is the fully qualified domain name of the KUMA Core server.
   - <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
   - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

     The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
     You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

     To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

   - <service_ID> is the service ID copied from the KUMA web interface.

   Example

```
sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --pair.fingerprint XXXXX --id XXXXX
--install
```

   When deploying several KUMA services on the same node, during the installation process you must specify unique ports for each component using the `--api.port <port>` option. The following setting values are used by default: `--api.port 7221`. Only one storage service can be installed per node.

3. Repeat steps 1–2 for each storage service.

   The storage is installed.

The storage service can be started if IPv6 and IPv4 formats are allowed. If you only use IPv4, specify the following in the `override configuration` field of the storage resource:

```
<interserver_listen_host>0.0.0.0</interserver_listen_host>
```

For the storage service to work correctly, the server node name must match one of its IP addresses. Review the `/etc/hosts` file to make sure it matches. To view the list of local IP addresses, use the following command:

```
ip a
```

Once settings of a storage are changed, its service must be restarted.

Viewing storage partitions

After creating and installing a storage service, you can view its partitions and, if necessary, delete them.

Viewing storage partitions

To view the storage partitions:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check box next to the storage whose partitions you want to view.
3. In the toolbar or the menu (⋮), click **Go to partitions**.

   The storage partition table opens. When viewing, you can switch between the **Hot storage** and **Cold storage** tabs.

You can sort the table by tenant, partition creation date, partition name, partition size, cold storage start date, and data retention end date by clicking the sort icon ⌄ in the column header and selecting **Ascending** or **Descending**.

The resource table contains the following columns:

- **Tenant** is the name of the tenant that owns the stored data. You can filter the table by specific tenants. To do this, click the column header and select the check boxes next to the relevant tenants.
- **Created** is the partition creation date.
- **Space** is the name of the space. You can filter the table by specific partitions. To do this, click the column header and select the check boxes next to the relevant partitions.
- **Size** is the size of the space. By clicking the column header, you can choose to display data in bytes, megabytes, gigabytes, or terabytes.
- **Events** is the number of stored events.
- **Transfer to cold storage** is the date when data will be migrated from the ClickHouse clusters to cold storage disks.
- **Expires** is the date when the partition expires. After this date, the partition and the events it contains are no longer available.

Deleting storage partitions

> You cannot delete partitions for audit events.

To delete a partition:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check box next to the storage whose partitions you want to view.
3. In the toolbar or the menu (⋮), click **Go to partitions**.
4. In the storage partitions table, select the check box next to the relevant partition and click **Delete**.
   A confirmation window opens.
5. Click **OK**.

The partition is deleted.

Viewing active queries in ClickHouse

You can view and cancel queries from other users and KUMA resources that are currently being executed.

> To view and cancel queries, a user account with General administrator rights is required.

Viewing the active queries

To view the table of active queries:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check boxes next to the relevant storages.
3. In the toolbar or in the menu (⋮), click **Active queries**.

   This opens the table with active queries to ClickHouse. If you have selected multiple storages, the table displays active queries from each selected storage.

You can sort the table by clicking the sort icon ⌄ in the column header and selecting **Ascending** or **Descending**.

The resource table contains the following columns:

- **Started** is the date and time when the query was initiated.
- **Created by** is the initiator of the query. For user queries, the KUMA user name is displayed. For queries of the **Resource** type, the resource name is displayed.
- **Query** is the text of the SQL query executed in ClickHouse.
- **Type** is the type of the query:
  - **In background** indicates that the query was initiated by the user in the background using the **Run in background** button.
  - **Resource** indicates an internal SQL query initiated by a KUMA resource, for example, during data processing or analysis.
  - **User** indicates an SQL query initiated by the user by clicking the **Run query** button and executed normally.
- **Storage** is the name of the ClickHouse storage where the query is being executed.

If necessary, you can customize the columns by clicking the gear icon. To update data, click the update icon.

Canceling queries

To cancel running queries:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check boxes next to the relevant storages.
3. In the toolbar or in the menu (⋮), click **Active queries**.
4. In the table, select the check boxes next to one or more queries that you want to cancel, and click **Cancel query**.

   A confirmation window opens.
5. If necessary, in the **Specify a reason** field, specify the reason for canceling the queries.
6. Click **OK**.

The queries are canceled and deleted from the table. An audit event is automatically generated.

Cold storage of events

In Kaspersky SIEM, you can configure migration of legacy data from a ClickHouse cluster to a cold storage. Cold storage can be implemented using the local disks mounted in the operating system, a Hadoop Distributed File System (HDFS), or an S3 cloud storage (Simple Storage Service).

Starting with KUMA version 4.2, we no longer recommend using HDFS as cold storage. Support for the HDFS file system will be discontinued in a future release. Users that use HDFS are advised to plan a migration to S3.

Cold storage functionality is enabled when at least one cold storage disk was specified during storage creation. If multiple storages are used, a cold storage disk or a HDFS or S3 disk must be mounted at the path specified in the storage configuration on each node with data.

The storage service may fail and cannot be started again in the following cases:

- Cold storage disk is not configured and the server runs out of disk space in a hot storage.
- Cold storage disk is configured and runs out of space.
- Cluster cannot gain access to the configured cold storage disk.

To avoid such situations, we recommend adding custom conditions for storing events in hot storage.

You can add cold storage disks when creating a storage resource set, or you can remove them. If you have added multiple cold storage disks, data is written to them in a round-robin manner. If data to be written to disk would take up more space than is available on that disk, this data and all subsequent data is written round-robin to the next cold storage disks. If you added only two cold storage disks, the data is written to the drive that has free space left.

After changing the cold storage settings, the storage service must be restarted. If the service does not start, the reason is indicated in the storage log.
The storage service must also be restarted if the path to the S3 storage was specified incorrectly. Note that the created `storage.xml` file is not automatically deleted. You need to manually clear the `/opt/kaspersky/kuma/clickhouse/cfg/config.d/` folder and configure cold storage again.

If the cold storage disk specified in the storage settings has become unavailable (for example, out of order), this may lead to errors in the operation of the storage service. In this case, recreate a disk with the same path (for local disks) or the same address (for HDFS and S3 disks) and then remove it from the storage settings.

Rules for moving the data to the cold storage disks

You can configure the storage conditions for events in hot storage of the ClickHouse cluster by setting a limit based on retention time or on maximum storage size. When cold storage is used, every 15 minutes and after each KUMA Core restart, Kaspersky SIEM checks if specified storage conditions are met:

1. Kaspersky SIEM gets partitions for the storage being checked and groups them by cold storage disks and spaces.

2. For each space, Kaspersky SIEM checks whether a specified storage condition is met.

3. If the condition is met (for example, if the space contains events that exceed their retention time, or if the size of the storage has reached or exceeded limit specified in the condition), Kaspersky SIEM transfers all partitions with the oldest date to cold storage disks or deletes these partitions if no cold storage disk is configured or if it is configured incorrectly. This action is repeated while the configured storage condition remains satisfied in the space; for example, if after deleting partitions for a date, the storage size still exceeds the maximum size specified in the condition.

   Kaspersky SIEM generates an audit event when data transfer starts and ends, or when data is deleted.

   Moving and processing of events is done at the partition level. For more information on managing partitions, see the section Disconnecting, archiving, and connecting partitions.

4. If retention time is configured in Kaspersky SIEM, whenever partitions are transferred to cold storage disks, a check is made to ensure that the specified conditions are met on the disk. If events are found on the disk that have been stored for longer than the **Event retention time**, which is counted from the moment the events were received by Kaspersky SIEM, the solution deletes these events or all partitions for the oldest date.

   Kaspersky SIEM generates audit events when data is deleted.

If the disks of the ClickHouse cluster are 97% full, the largest partitions are either automatically transferred to cold storage disks, or deleted if there are no cold storage disks.

During data transfer, the storage service remains operational, and its status stays green in the **Resources** → **Active services** section. When you hover over the status icon, a message is displayed about the data transfer. When a cold storage disk is removed, the storage service has the yellow status.

Special considerations for storing and accessing events

- When using HDFS drives for cold storage, you must ensure data protection in one of the following ways:

  - Configure a separate physical interface in the VLAN, where only HDFS disks and the ClickHouse cluster are located.

  - Configure network segmentation and traffic filtering rules that exclude direct access to the HDFS disk or interception of traffic to the disk from ClickHouse.

- Events located in the ClickHouse cluster and on the cold storage disks are equally available in the Kaspersky SIEM web interface. For example, when you search for events or view events related to alerts.

- You can disable the storage of events or audit events on cold storage disks. To do this, do the following in the storage settings:
  - If you do not want to store events on cold storage disks, do one of the following:
    - If in the **Retention policy options** field, you have selected a gigabyte or percentage based storage condition, in the **Events storage time** field, specify `0`.
    - If in the **Retention policy options** field, you have selected a storage condition in days, in the **Event storage time** field, specify the same number of days as in the **Retention policy options**.
  - If you do not want to store audit events on cold storage disks, in the **Audit cold retention period** field, specify `0` (days).

Special considerations for using HDFS disks

- Before connecting HDFS disks, create directories for each node of the ClickHouse cluster on them in the following format: `<HDFS disk host>/<shard ID>/<replica ID>`. For example, if a cluster consists of two nodes containing two replicas of the same shard, the following directories must be created:
  - `hdfs://hdfs-example-1:9000/clickhouse/1/1/`
  - `hdfs://hdfs-example-1:9000/clickhouse/1/2/`

  Events from the ClickHouse cluster nodes are migrated to the directories with names containing the IDs of their shard and replica. If you change these node settings without creating a corresponding directory on the HDFS disk, events may be lost during migration.
- HDFS disks added to storage operate in the JBOD mode. This means that if one of the disks fails, access to the storage will be lost. When using HDFS, take high availability into account and configure RAID, as well as storage of data from different replicas on different devices.
- The speed of event recording to HDFS is usually lower than the speed of event recording to local disks. The speed of accessing events in HDFS, as a rule, is significantly lower than the speed of accessing events on local disks. When using local disks and HDFS disks at the same time, the data is written to them in turn.
- HDFS is used only as distributed file data storage of ClickHouse. Compression mechanisms of ClickHouse, not HDFS, are used to compress data.
- The ClickHouse server must have write access to the corresponding HDFS storage.

Removing cold storage disks

Before physically disconnecting cold storage disks, remove these disks from the storage settings.

To remove a disk from the storage settings:

1. In the web interface, go to the **Resources** → **Storages** section and select the storage.

2. In the window that opens, in the **Disks for cold storage** settings section, in the required disk settings section, click the X icon to remove the disk.

3. In the confirmation window, click **OK**.

   Data from removed disk is automatically migrated to other cold storage disks or, if there are no such disks, to the ClickHouse cluster. While data is being migrated, the status icon of the storage turns yellow and an hourglass icon is displayed. Audit events are generated when data transfer starts and ends.

   After event migration is complete, the disk is automatically removed from the storage settings. It can now be safely disconnected.

Removed disks can still contain events. If you want to delete them, you can delete the data partitions manually using the following command:

```
ROP PARTITION
```

If the cold storage disk specified in the storage settings has become unavailable (for example, out of order), this may lead to errors in the operation of the storage service. In this case, create a disk with the same path (for local disks) or the same address (for HDFS and S3 disks) and then remove it from the storage settings.

Detaching, archiving, and attaching partitions

If you want to optimize disk space and speed up queries in KUMA, you can detach data partitions in ClickHouse, archive partitions, or move partitions to a drive. If necessary, you can later reattach the partitions you need and perform data processing.

You can also use the created partition archives as backup copies of these partitions.

Detaching partitions

To disconnect partitions:

1. Select the shard on all replicas of which you want to disable the partition.

2. Get the partition ID using the following command:

   ```
   sudo /opt/kaspersky/kuma/storage/<storage ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   In this example, the command returns the partition ID for November 30, 2023.

3. One each replica of the shard, detach the partition using the following command and specifying the received ID:

```
sudo /opt/kaspersky/kuma/storage/<storage ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<partition ID>'"
```

The partition is disabled on all replicas of the shard. Now you can move data to a drive or archive the partition.

Archiving partitions

To archive detached partitions:

1. Find the detached partition in disk subsystem of the server:

```
sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <ID of the detached partition>\*
```

2. Go to the `detached` directory with a disconnected partition and do the archiving:

```
sudo cd <path to the detached directory containing the detached partition>
sudo zip -9 -r detached.zip *
```

Example

```
sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
sudo zip -9 -r detached.zip *
```

The partition is archived.

Attaching partitions

To connect archive partitions to the solution:

1. In the web interface, open the **Resources** → **Storage** section and in the settings of the used storage, increase the value of the **Event retention time** setting.

   Data is deleted according to the date specified in the Timestamp field (when the event was received) and according to the value of the **Event retention time** setting that you specified for the storage.

   Before restoring archived data, make sure that the **Event storage period** value is greater than the date in the "Timestamp" field. If this is not the case, the archived data will be deleted within 1 hour.

2. Place the archive partition into the `detached` directory of your storage, and extract the archive:

```
sudo unzip detached.zip -d <path to the detached directory>
```

Example

```
sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
```

3. Connect the partition using the command:

```
sudo /opt/kaspersky/kuma/storage/<storage ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<partition ID>'"
```

4. Repeat the steps of extracting the archive and attaching the partition on each replica of the shard.

   The archived partition is attached and its events are again available for search.

Scheduling partition backup

> Only users with the General administrator role may configure scheduled backup of partitions.

You can configure and use partition backup and event cold storage at the same time. If necessary, you can use a backup copy to restore partitions.

To schedule backup:

1. In the web interface, go to the **Resources and services** → **Active services** section.

   If necessary, in the table that opens, in the **Type** column, select **Storage**.

2. Go to active storage to configure the settings. To do this, in the **Service** column, click the storage name.

3. In the **Edit storage** window that opens, on the **Basic settings** tab, in the **Backup and recovery settings** section, manage the following settings:

   a. In the **Storage backup** field, specify the path used to save the backup file, e.g. `/mnt/data`.

      Path requirements:

      - The path must exist and be the same on all nodes of the storage cluster.
      - The user must have read, write, and execute permissions in the specified directory.
      - The specified directory must belong to the second or deeper nesting level. Using a directory at the first nesting level, for example `/backup` is not allowed.
      - The directory name may not contain a period.
      - **The path must not contain the following prefixes**.

        Prefixes that cannot be used when specifying paths to files:

        - `/*`
        - `/bin`
        - `/boot`
        - `/dev`
        - `/etc`

- `/home`
- `/lib`
- `/lib64`
- `/proc`
- `/root`
- `/run`
- `/sys`
- `/tmp`
- `/usr/*`
- `/usr/bin/`
- `/usr/local/*`
- `/usr/local/sbin/`
- `/usr/local/bin/`
- `/usr/sbin/`
- `/usr/lib/`
- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path.

Files are available at the following paths:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

Make sure that the user has access rights for the specified directory. If no path is specified, performing the backup is impossible.

b. Enable the **Add automatic backup** toggle switch.

c. In the **Back up after several days** field, specify an integer number of days after the creation of a partition after which you want a backup copy to be created. For example, if the value is **1**, backup is performed for the partition created the day before yesterday.

d. In the **Replicas** drop-down list, select one replica that you want to back up. Selecting multiple replicas of the same shard causes data duplication.

   If multiple shards are used in the cluster, the **Replicas** list contains only those replicas whose IDs are specified in all shards.

4. Under **Partitions**, click **Add partition** and manage the following settings:

   a. In the **Tenant** drop-down list, select the tenant that contains the partition that you want to back up.

   b. In the **Spaces** drop-down list, select one or more storage spaces that belong to the partition that you want to back up. If no value is specified, the whole partition is backed up.

   You can manage settings for multiple partitions. To do this, click **Add partition** and configure the settings in the displayed fields. For example, if you want to back up the **Audit** space and you have 10 tenants, you must configure the backup separately for each tenant.

5. Click **Save**.

   Once the settings are saved, the `backup` and `restore` directories are automatically created at the specified path. Subdirectories with tenant ID and space ID are automatically created in the `backup` directory. For example, if you specify `/mnt/data` as the backup saving path, the full path to the backup file will look like `/mnt/data/backup/<tenant ID>/<storage space ID>/<partition creation date>.zip`. You can find the tenant or space ID in the **Events** section of the event card.

The scheduled partition backup will be configured. After the backup of the partitions is started, the corresponding task and audit event are created. If a backup fails, the storage service gets the yellow status in the **Active services** section, and an error message is displayed when you hover over the yellow status indicator. The next time a scheduled backup is started, an attempt is made to back up the old data first.

Manually backing up partitions

> Only users with the General administrator role may configure scheduled backup of partitions.

You can configure and use partition backup and event cold storage at the same time. If necessary, you can use a backup copy to restore partitions.

To manually create a backup copy of a partition:

1. In the web interface, open the **Resources** → **Active services** section.

   If necessary, in the table that opens, in the **Type** column, select **Storage**.

2. Go to active storage to configure the settings. To do this, in the **Service** column, click the storage name.

3. In the **Edit storage** window that opens, go to the **General settings** tab.

4. In the **Configure backup and restore** section, in the **Storage backup** field, specify the path for storing the backup file, for example, `/mnt/data`.

Path requirements:

- The path must exist and be the same on all nodes of the storage cluster.
- The user must have read, write, and execute permissions in the specified directory.
- The specified directory must belong to the second or deeper nesting level. Using a directory at the first nesting level, for example `/backup` is not allowed.
- The directory name may not contain a period.
- **The path must not contain the following prefixes**.

  Prefixes that cannot be used when specifying paths to files:

  - `/*`
  - `/bin`
  - `/boot`
  - `/dev`
  - `/etc`
  - `/home`
  - `/lib`
  - `/lib64`
  - `/proc`
  - `/root`
  - `/run`
  - `/sys`
  - `/tmp`
  - `/usr/*`
  - `/usr/bin/`
  - `/usr/local/*`
  - `/usr/local/sbin/`
  - `/usr/local/bin/`
  - `/usr/sbin/`
  - `/usr/lib/`

- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path.

Files are available at the following paths:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

5. Save your changes.
6. In the **Resources** → **Active services** section, select the check box next to the storage service with a green status.
7. In the toolbar or menu (⋮), select **Backup** and click **Create a backup copy**.

   The **Create a backup copy** option is available, if one storage service with a green status is selected.

   The option is not available in the following cases:

   - You have selected the check boxes next to several services.
   - Storage service has a red status.
   - No check boxes are selected.
   - You have selected a check box next to a service of another type.
8. In the **Partition backup** window that is opened, manage the following settings:

   a. In the **Tenant** drop-down list, select the tenant that contains the partition that you want to back up.

   b. In the **Spaces** drop-down list, select one or more storage spaces that belong to the partition that you want to back up. If no value is specified, the whole partition is backed up.

   c. In the **Replicas** drop-down list, select one replica or all replicas that you want to back up. Selecting multiple replicas of the same shard causes data duplication.

   d. In the **Date range** field, use the calendar to specify the date range for the partitions to be included in the backup.
9. Click **OK**.
10. In the confirmation window, click **OK**.

Once the settings are saved, the `backup` and `restore` directories are automatically created at the specified path. Subdirectories with tenant ID and space ID are automatically created in the `backup` directory. For example, if you specify `/mnt/data` as the backup saving path, the full path to the backup file will look like `/mnt/data/backup/<tenant ID>/<storage space ID>/<partition creation date>.zip`. If you need to look up the ID of a tenant or space, go to the **Events** section, open the event card and view the information that you need.

If the file name for manual backup is the same as the name of the scheduled backup file, an error is returned stating that the backup file cannot be saved. You need to rename or delete the file, and perform the manual backup again.

Manual backup of partitions will be completed. After the backup of the partitions is started, the corresponding task and audit event are created. If a backup fails, the storage service gets the yellow status in the **Active services** section, and an error message is displayed when you hover over the yellow status indicator.

Restoring partitions from backup

Only users with the General administrator role may restore partitions from backup.

To restore a partition from backup:

1. Move the ZIP file of the backup copy from the `backup` directory to the `restore` directory.
2. Grant the KUMA user permissions to the backup copy ZIP file in the `restore` directory using the following command:

   ```
   sudo chown kuma *.zip
   ```

3. In the **Resources** → **Active services** section of the web interface, select the check box next to the storage service with a green status.
4. In the toolbar or menu (⋮), select **Backup** → **Restore**.
5. In the **Restore from the current KUMA installation** window that opens, in the **Replicas** drop-down list, select one replica in which you want to perform restoration from backup.
6. Click **OK**.
7. In the confirmation window, click **OK**.

Partitions will be restored from the backup. The corresponding task and audit event are also created.

Importing partitions from a third-party instance of Kaspersky SIEM

Import of partitions from an external Kaspersky SIEM instance is available to the users with the General administrator role.

To import partitions from a third-party instance of Kaspersky SIEM:

1. Place the ZIP file from which you want to import partitions into the `restore` directory. Partitions will be imported from this directory.

2. Grant the KUMA user permissions to the backup copy ZIP file in the `restore` directory using the following command:

   ```
   sudo chown kuma *.zip
   ```

3. In the **Resources** → **Active services** section of the web interface, select the check box next to the storage service with a green status.

4. In the toolbar or menu (⋮), select **Backup** → **Import**.

5. In the **Import from an external installation of KUMA** window, perform the following actions:

   a. In the **Tenant** drop-down list, select the tenant for which partitions will be imported.

   b. In the **Replicas** drop-down list, select one replica to which the partitions will be imported.

   c. In the **Fields for exclusions** drop-down list, select the check boxes next to the fields to be deleted during import.

   By default, the check boxes are selected for the following fields:

   - AggregationRuleName
   - CorrelationRuleName
   - SourceAccountID
   - DestinationAccountID
   - SourceAssetID
   - DestinationAssetID
   - DeviceAssetID
   - KUMA extended event schema fields:
     - Extended event schema fields (SA., F., N., and others).
     - KSC asset fields
     - KLCorrelationRulePriority = "KL_CorrelationRulePriority"
     - KLSourceAssetDisplayName = "KL_SourceAssetDisplayName"
     - KLDestinationAssetDisplayName = "KL_DestinationAssetDisplayName"
     - KLDeviceAssetDisplayName = "KL_DeviceAssetDisplayName"
     - KLSourceAccountDisplayName = "KL_SourceAccountDisplayName"

- KLDestinationAccountDisplayName = "KL_DestinationAccountDisplayName"
- KLDllHijackingResult = "KL_AI_DLLHijackingCheckResult"

When you select the **KUMA extended event schema fields** group, the whole group of fields is removed. You cannot remove fields partially.

By default, the following fields are removed and therefore not available for selection in the web interface:

- ServiceID
- ServiceName
- CorrelationRuleID
- AggregationRuleID

6. Click **OK**.
7. In the confirmation window, click **OK**.

Partitions from a third-party instance of Kaspersky SIEM are imported. A partition import task and an audit event are also created.

Configuring retention periods and priority deletion of events

If Kaspersky SIEM receives events for which different retention periods are set, such events must be distributed to to different storage spaces. For each space, you need to specify a filter that determines which events go into the space and how they must be stored.

If the storage lacks free space, events with a short retention period can be deleted before the data that need to be stored for longer. To achieve this, you need to specify a condition for disk space running out for the space containing such events.

To configure retention periods and priority deletion of events:

1. In the KUMA web interface, go to the **Resources** → **Storages** section.
2. Create a new storage or open the settings of an existing storage.
3. Under **Spaces**, click the **Add space** button and specify the following settings for the first space:
   a. In the **Name** field, specify `retention_180`.
   b. Under **Retention policy options**, select **Days** in the drop-down list and specify `180`.
   c. Under **Filter parameters**, select or create a filter that selects events that must be retained for 180 days.

4. Click the **Add space** button and specify the following settings for the second space:

   a. In the **Name** field, specify `retention_90`.

   b. Under **Retention policy options**, select **Days** in the drop-down list and specify `90`.

   c. Under **Filter parameters**, select or create a filter that selects events that must be retained for 90 days.

5. Click the **Add space** button and specify the following settings for the third space:

   a. In the **Name** field, specify `netflow`.

   b. Under `Retention policy options`, select **Days** in the drop-down list and specify `30`.

   c. Click the **Add policy options** button.

   d. In the drop-down list, select **Percent** and specify `95`.

   e. Under **Filter parameters**, select or create a filter with the `DeviceProduct=netflow` condition.

   As a result, two storage conditions are configured for the netflow space: the event retention period is 30 days, and the disk space limit is 95%.

6. Click the **Save** button.

7. After creating and configuring spaces, submit test events for each group and verify that they end up in the appropriate spaces.

Make sure that the following conditions are met:

- Events from the retention_180 space are deleted after 180 days of retention.
- Events from the retention_90 space are deleted after 90 days of retention.
- Events from the NetFlow space are deleted after 30 days of retention; also, when the disk space limit is reached, space is freed up by deleting older events from the space.

Events are routed to spaces in accordance with the configured filters and are retained for the specified period. If the storage becomes full before the configured limit, old NetFlow events are prioritized for deletion, which means that data with longer retention periods is retained for longer.

Event reception and normalization

A *collector* is a component of the solution that receives events from event sources, process the events, and transmit them to other components of the solution. During processing, the collector performs normalization of events, and can also apply filtering, enrichment, conversion and aggregation of data. After processing, events are sent to the configured destinations.

The maximum size of an event that can be processed by the KUMA collector is 4 MB.

> If you are using the SMB license, and both the hourly average EPS and the daily average EPS allowed by the license is exceeded for a collector, the collector stops receiving events and is displayed with a red status and a notification about the EPS limit being exceeded. The user with the General Administrator role gets a notification about the EPS limit being exceeded and the collector being stopped. Every hour, the hourly average EPS value is recalculated and compared with the EPS limit in the license. If the hourly average is under the limit, the restrictions on the collector are lifted, and the collector resumes receiving and processing events.

For each collector, one connector and one normalizer must be configured. You can also configure any number of additional normalizers, filters, enrichment rules, and aggregation rules. For the collector to send normalized events to other services, you must add destinations. Normally, two destinations are used: a storage and a correlator.

A collector receives raw events from event sources, performs normalization, and sends processed events to their destinations.

Predefined collectors

The KUMA distribution kit includes the following predefined collectors:

- [OOTB] CEF collects CEF events received over the TCP protocol.
- [OOTB] KSC collects events from Kaspersky Security Center over the Syslog TCP protocol.
- [OOTB] KSC SQL collects events from Kaspersky Security Center using an MS SQL database query.
- [OOTB] Syslog collects events via the Syslog protocol.
- [OOTB] Syslog-CEF collects CEF events that arrive over the UDP protocol and have a Syslog header.

Recommendations for collector resources

For efficient event processing, a CPU's core count is more important than its clock rate. For example, eight CPU cores with a medium clock rate will process events more efficiently than four CPU cores with a high clock rate.

Consider also that the amount of RAM utilized by the collector depends on configured enrichment methods (DNS, accounts, assets, enrichment with data from Kaspersky CyberTrace) and whether aggregation is used (RAM consumption is influenced by the data aggregation window setting, the number of fields used for aggregation of data, volume of data in fields being aggregated). The utilization of computation resources by KUMA depends on the type of events being parsed and the efficiency of the normalizer.

For example, with an event stream of 1000 EPS and event enrichment disabled (event enrichment is disabled, event aggregation is disabled, 5000 accounts, 5000 assets per tenant), one collector requires the following resources:

- 1 CPU core or 1 virtual CPU
- 512 MB of RAM
- 1 GB of free disk space (not counting event cache).

For example, to support five collectors that do not perform event enrichment, you need to allocate the following resources: 5 CPU cores, 2.5 GB of RAM, and 5 GB of free disk space.

Algorithm of collector operation

The collector iterates over the following steps:

1 Receive messages from event sources

The collector receives messages from event sources through connectors. Depending on the type of connector, data can be received in two ways:

- a passive connector waits for incoming events from the source;
- an active connector independently initiates a connection to the source.

The connector type is determined by the transport protocol used for data exchange.

2 Event parsing and normalization

Received messages are processed by the normalizer and normalization rules. During processing, data is converted from the original format to a unified event representation. The normalizer used is determined by the format of incoming messages.

3 Filtering of normalized events

Normalized events are checked against the filter conditions. Events that match the specified conditions are sent to the subsequent processing stages.

4 Enrichment and conversion of normalized events

At the enrichment stage, events are supplemented with data from internal and external sources.

At the conversion stage, the values of the event fields are modified according to the defined conversion rules.

5 Aggregate normalized events

Similar events can be merged into a single aggregated event in accordance with the aggregation rules. This helps reduce the volume of data sent and stored, lower the load on further processing services, and decrease consumption of the license quota (EPS). For example, several events of network connections between two IP addresses received within a certain time interval can be merged into a single event.

6 Transferring normalized events

After all processing stages are completed, the event is sent to the configured destinations for further storage.

Supported event sources

KUMA supports the normalization of events coming from systems listed in the table below. Normalizers for these systems are included in the distribution kit.

Supported event sources

System name	Normalizer name	Type	Normalizer description
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	Designed for processing the event log of the 1C system. The event source is the 1C log.
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	Designed for processing the technology event log. The event source is the 1C technology log.
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
AhnLab UTM	[OOTB] Ahnlab UTM	regexp	Designed for processing events from the Ahnlab system. The event sources are system logs, operation logs, connections, the IPS module.
Alcatel AOS-W	[OOTB] Alcatel AOS-W syslog	regexp	Designed for processing some of the events received from Alcatel AOS-W 6.4 via Syslog.
Alcatel Network Switch	[OOTB] Alcatel Network Switch syslog	Syslog	Designed for processing events received from Alcatel network switches via Syslog.
Ansible	[OOTB] Ansible syslog	Syslog	Designed for processing events from Ansible 2.10.8 via Syslog.
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	Designed for processing events from the logs of the Apache Cassandra database version 4.0.
Apache Kafka	[OOTB] Apache Kafka syslog	regexp	Designed for processing Apache Kafka 3.8.1 system audit events received via Syslog.
Apache Tomcat	[OOTB] Apache Tomcat json	Syslog	Designed for processing events from the Apache Tomcat system (version 9.0 and later, 10.1 and later, 11.0 and later) via Syslog in JSON and key-value formats.
APC Smart-UPS	[OOTB] APC Smart UPS	regexp	Designed for processing APC Smart-UPS system audit events.

System name	Normalizer name	Type	Normalizer description
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Atlassian Confluence	[OOTB] Atlassian Jira Conflunce file	regexp	Designed for processing events of Atlassian Jira, Atlassian Confluence systems (Jira 9.12, Confluence 8.5) stored in files.
Atlassian Jira	[OOTB] Atlassian Jira Conflunce file	regexp	Designed for processing events of Atlassian Jira, Atlassian Confluence systems (Jira 9.12, Confluence 8.5) stored in files.
Avanpost FAM	[OOTB] Avanpost FAM syslog	regexp	Designed for processing events of the Avanpost Federated Access Manager (FAM) 1.9 received via Syslog.
Avanpost IDM	[OOTB] Avanpost IDM syslog	regexp	Designed for processing events of the Avanpost IDM system received via Syslog.
Avanpost PKI	[OOTB] Avanpost PKI syslog CEF	Syslog	Designed for processing events received from Avanpost PKI 6.0 in CEF format via Syslog.
Avaya Aura Communication Manager	[OOTB] Avaya Aura Communication Manager syslog	regexp	Designed for processing some of the events received from Avaya Aura Communication Manager 7.1 via Syslog.
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Arbor Pravail	[OOTB] Arbor Pravail syslog	Syslog	Designed for processing events of the Arbor Pravail system received via Syslog.
Aruba Aruba AOS-S	[OOTB] Aruba Aruba AOS-S syslog	regexp	Designed for processing events received from Aruba network devices with Aruba AOS-S 16.10 firmware via Syslog. The normalizer supports the following types of events: accounting events, ACL events, ARP protect events, authentication events, console events, loop protect events.
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway syslog	regexp	Designed for processing events from Barracuda Cloud Email Security Gateway via Syslog.
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway syslog	Syslog	Designed for processing some of the events received from Barracuda Web Security Gateway 15.0 via Syslog.
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
BeyondTrust BeyondInsight	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	Designed for processing events from the DDOS Mitigator protection system received via Syslog.
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.

System name	Normalizer name	Type	Normalizer description
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	Designed for processing events from the Symantec Endpoint Protection system.
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Brocade Fabric OS	[OOTB] Brocade Fabric OS syslog	Syslog	Designed for processing events of Brocade Fabric 9.1 received via syslog.
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	Designed for processing events received via Syslog from the Canonical LXD system version 5.18.
Check Point	[OOTB] Checkpoint syslog	Syslog	Designed for processing events received from the Check Point R81 firewall via the Syslog protocol.
Cisco Access Control Server (ACS)	[OOTB] Cisco ACS syslog	regexp	Designed for processing events of the Cisco Access Control Server (ACS) system received via Syslog.
Cisco ACE	[OOTB] Cisco ASA and IOS syslog	regexp	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco ASA	[OOTB] Cisco ASA and IOS syslog	Syslog	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	Designed for processing the event log of the Cisco Email Security Appliance (WSA) 14.2 proxy server, the access.log file.
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	Designed for processing certain types of events received from Cisco ESA 16.0 via Syslog.
Cisco Firepower Threat Defense	[OOTB] Cisco ASA and IOS syslog	Syslog	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco Firewall Services Module (FWSM)	[OOTB] Cisco ASA and IOS syslog	Syslog	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	Designed for processing events of the Cisco Identity Services Engine (ISE) system v3.2 received via Syslog.
Cisco IOS	[OOTB] Cisco ASA and IOS syslog	Syslog	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	Designed for processing events from Cisco Netflow version 5.
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	Designed for processing events from Cisco Netflow version 9.
Cisco Next-Generation Intrusion Prevention System (NGIPS)	[OOTB] Cisco ASA and IOS syslog	Syslog	Designed for processing audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco PIX	[OOTB] Cisco ASA and IOS syslog	regexp	Designed for processing types of audit events from Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE network devices and devices running Cisco IOS via Syslog.
Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	Designed for processing events of the Cisco Prime system version 3.10 received via Syslog.

System name	Normalizer name	Type	Normalizer description
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Cisco Unified Communications Manager	[OOTB] Cisco Unified Communications Manager	regexp	Designed for processing event types from Cisco Unified Communications Manager 11.5.1.
Cisco Wireless LAN Controllers (WLCs)	[OOTB] Cisco WLC syslog	regexp	Designed for processing events received from Cisco WLC network devices (2500 Series Wireless Controllers, 5500 Series Wireless Controllers, 8500 Series Wireless Controllers, Flex 7500 Series Wireless Controllers) via Syslog.
Cisco Web Security Appliance (WSA)	[OOTB] Cisco WSA file, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA file is a normalizer designed for processing the event log of the Cisco WSA proxy server (versions 14.2, 15.0). The normalizer supports processing events generated using the following template: %t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr %?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%. %) %q %k %u %m [OOTB] Cisco WSA syslog is a normalizer designed for processing events received from the Cisco WSA system (version 15.0) via Syslog.
Citrix NetScaler	[OOTB] Citrix NetScaler syslog	regexp	Designed for processing events received from the Citrix NetScaler 13.7 load balancer, Citrix ADC NS13.0.
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	Designed for processing events of the Codemaster Mirada system received via Syslog.
CollabNet Subversion Edge	[OOTB] CollabNet Subversion Edge syslog	Syslog	Designed for processing events received from the Subversion Edge (version 6.0.2) system via Syslog.
CommuniGate Pro	[OOTB] CommuniGate Pro	regexp	Contains a resource set for processing some of the events of the SIP module of the CommuniGate Pro system versions 6.1 and 6.5.1, transmitted by the KUMA agent via TCP. For details on configuring the collector, see Creating a collector.
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Cribl Stream	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
CrowdStrike Falcon	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	Designed for processing events of the CyberPeak Spektr system version 3 received via Syslog.
Cyberprotect Cyber Backup	[OOTB] Cyberprotect Cyber Backup SQL [OOTB] Cyberprotect Cyber Backup syslog	sql, regexp	[OOTB] Cyberprotect Cyber Backup SQL is a normalizer designed to process events received by the connector from the database of the Cyber Backup system (version 16.5). [OOTB] Cyberprotect Cyber Backup syslog is a normalizer designed to process events received from the Cyber Backup system (version 17.2, 17.3, 18.5) via Syslog in CEF format.

System name	Normalizer name	Type	Normalizer description
Deep Instinct	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Dell Network Switch	[OOTB] Dell Network Switch syslog	regexp	Designed for processing events received from Dell network switches via Syslog.
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
D-Link Switches	[OOTB] D-Link Switches	regexp	Designed for processing events from D-Link switches (DES-2108, DES-3200-28, DES-3828, DES-3800) via Syslog.
BIND DNS server	[OOTB] BIND Syslog [OOTB] BIND file	Syslog regexp	[OOTB] BIND Syslog is designed for processing events of the BIND DNS server received via Syslog. [OOTB] BIND file is designed for processing event logs of the BIND DNS server.
Docsvision	[OOTB] Docsvision syslog	Syslog	Designed for processing audit events received from the Docsvision system via Syslog.
Dovecot	[OOTB] Dovecot Syslog	Syslog	Designed for processing events of the Dovecot mail server received via Syslog. The event source is POP3/IMAP logs.
Dragos Platform	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Dr.Web Enterprise Security Suite	[OOTB] Syslog-CEF	Syslog	Designed for processing Dr.Web Enterprise Security Suite 13.0.1 events in the CEF format.
EclecticIQ Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Eltex ESR	[OOTB] Eltex ESR syslog	Syslog	Designed to process part of the events received from Eltex ESR network devices via Syslog.
Eltex MES	[OOTB] Eltex MES syslog	regexp	Designed for processing events received from Eltex MES network devices via Syslog (supported device models: MES14xx, MES24xx, MES3708P).
ESET PROTECT	[OOTB] ESET Protect syslog CEF	Syslog	Designed for processing events received in the CEF format received from the ESET PROTECT system (version 11.0) via Syslog. This package is available for KUMA version 3.2 or later.
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	Designed for processing of audit events of the Extreme Networks Summit Wireless Controller (model: WM3700, firmware version: 5.5.5.0-018R).
Factor-TS Dionis NX	[OOTB] Factor-TS Dionis NX syslog	regexp	Designed for processing audit events received from the Dionis-NX system (version 2.0.3) via Syslog.
F5 Advanced Web Application Firewall	[OOTB] F5 Advanced Web Application Firewall syslog	regexp	Designed for processing audit events received from the F5 Advanced Web Application Firewall system via Syslog.
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.

System name	Normalizer name	Type	Normalizer description
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Flant Deckhouse	[OOTB] Flant Deckhouse json	json	Designed for processing Metadata level audit events from Deckhouse (version 1.67) in JSON format.
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	Syslog	Designed for processing events received from Fortinet FortiAnalyzer 7.0, 7.2 via Syslog in CEF format.
Fortinet FortiADC	[OOTB] FortiADC syslog KV	regexp	Designed for processing event types received from Fortinet FortiADC 7.1 load balancers via Syslog in key-value format.
Fortinet FortiGate	[OOTB] FortiGate syslog KV [OOTB] FortiGate syslog CEF	regexp	The [OOTB] FortiGate syslog KV normalizer is designed for processing events received from FortiGate firewalls (version 7.0, 7.2) via syslog. The event source is FortiGate logs in key-value format. The [OOTB] FortiGate syslog CEF normalizer is designed for processing events received from Fortinet FortiGate (FortiOS 6.4) via syslog in CEF format.
Fortinet FortiMail	[OOTB] Fortimail	regexp	Designed for processing events of the FortiMail email protection system. The event source is FortiMail mail system logs.
Fortinet FortiPAM	[OOTB] Fortinet FortiPAM syslog	regexp	Designed for processing events from Fortinet FortiPAM system (version 7.4) in key-value format via Syslog.
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Fortinet FortiWeb	[OOTB] FortiNet FortiWeb CEF	Syslog	Designed for processing events from the Fortinet FortiWeb 7.6.1 system in CEF format.
FreeBSD	[OOTB] FreeBSD file	regexp	Designed for processing events of the FreeBSD operating system (version 13.1-RELEASE) stored in a file. The normalizer can process files produced by the praudit utility. Example: praudit -xl /var/audit/AUDITFILE >> file_name.log
FreeIPA	[OOTB] FreeIPA	json	Designed for processing events from the FreeIPA system. The event source is FreeIPA directory service logs.
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	Designed for processing events of the FreeRADIUS system received via Syslog. The normalizer supports events from FreeRADIUS version 3.0.
GajShield Firewall	[OOTB] GajShield Firewall syslog	regexp	Designed for processing part of the events received from the GajShield Firewall version GAJ_OS_Bulwark_Firmware_v4.35 via Syslog.
Garda Monitor	[OOTB] Garda Monitor syslog	Syslog	Designed for processing events of the Garda Monitor system version 3.4 received via Syslog.
Gardatech Garda DB	[OOTB] Gardatech GardaDB syslog	Syslog	Designed for processing events of the Gardatech Perimeter system version 5.3, 5.4 received via Syslog.
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	Designed for processing events of the Gardatech Perimeter system version 5.3 received via Syslog.
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Grafana	[OOTB] Grafana syslog json	Syslog	Designed for processing events from Grafana 9.5.15 in JSON format via Syslog.
HAProxy	[OOTB] HAProxy syslog	Syslog	Designed for processing events received from HAProxy 2.4 via Syslog. This normalizer supports events in the Default, TCP, TCP CLF (version 3.2 and later), HTTP, HTTP CLF, HTTPS (2.6 and later), and Error formats.
HashiCorp Vault	[OOTB] HashiCorp Vault json	json	Designed for processing events received from the HashiCorp Vault system version 1.16 in JSON format. The normalizer package is available in KUMA 3.0 and later.

System name	Normalizer name	Type	Normalizer description
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	Designed for processing events from Huawei Eudemon firewalls. The event source is logs of Huawei Eudemon firewalls.
Huawei iManager 2000	[OOTB] Huawei iManager 2000 file	regexp	Designed for processing of some of the events of the Huawei iManager 2000 system, which are stored in the \client\logs\rpc, \client\logs\deploy\ossDeployment files.
Huawei USG	[OOTB] Huawei USG Basic	Syslog	Designed for processing events received from Huawei USG security gateways via Syslog.
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	Designed for processing Huawei VRP events received via Syslog. The normalizer makes a partial selection of event data. The normalizer is available in KUMA 3.0 and later.
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Ideco UTM	[OOTB] Ideco UTM Syslog	Syslog	Designed for processing events received from Ideco UTM via Syslog. The normalizer supports events of Ideco UTM 14.7, 14.10, 17.5.
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Indeed Access Manager	[OOTB] Indeed Access Manager syslog	Syslog	Designed for processing events received from the Indeed Access Manager system via Syslog.
Indeed Privileged Access Manager	[OOTB] Indeed PAM syslog [OOTB] Indeed PAM syslog CEF	Syslog	The [OOTB] Indeed PAM syslog normalizer is designed to process events received from the Indeed Privileged Access Manager version 2.6. The [OOTB] Indeed PAM syslog CEF normalizer is designed to process events received from the Indeed Privileged Access Manager (version 3.3) in the CEF format via Syslog.
Indeed SSO	[OOTB] Indeed SSO xml	xml	Designed for processing events of the Indeed SSO (Single Sign-On) system. The normalizer supports KUMA 2.1.3 and later.
InfoWatch Person Monitor	[OOTB] InfoWatch Person Monitor SQL	sql	Designed for processing system audit events from the MS SQL database of InfoWatch Person Monitor 10.2.
InfoWatch Traffic Monitor	[OOTB] InfoWatch Traffic Monitor SQL	sql	Designed for processing events received by the connector from the database of the InfoWatch Traffic Monitor system.
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
IPFIX	[OOTB] IPFIX	ipfix	Designed for processing events in the IP Flow Information Export (IPFIX) format.
Juniper JUNOS	[OOTB] Juniper-JUNOS	regexp	Normalizer for Juniper JUNOS (version 24.2) events received via Syslog.
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	Designed for processing alerts or events from the Kaspersky Anti Targeted Attack activity log.
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	Designed for processing Kaspersky CyberTrace events.
Kaspersky DFI	[OOTB] Kaspersky DFI json	json	Designed for processing audit events of the Kaspersky DFI system in JSON format. The normalizer supports the processing of events generated by the "dfi" KUMA connector. Available in the resource set for KUMA 4.0 and later.
Kaspersky Endpoint Detection and Response (KEDR)	[OOTB] KEDR telemetry	json	Designed for processing Kaspersky EDR telemetry tagged by KATA. The event source is kafka, EnrichedEventTopic.

System name	Normalizer name	Type	Normalizer description
Kaspersky Endpoint Security for Linux	[OOTB] KESL syslog cef [OOTB] KESL json	Syslog, json	The [OOTB] KESL syslog cef normalizer is designed for processing events from Kaspersky Endpoint Security for Linux (KESL) 12.2 in CEF format via syslog. The [OOTB] KESL json normalizer is designed for processing events from Kaspersky Endpoint Security for Linux (KESL) 12.5 in JSON format.
KICS/KATA	[OOTB] KICS4Net v2.x	cef	Designed for processing KICS/KATA version 2.x events.
KICS/KATA	[OOTB] KICS4Net v3.x	Syslog	Designed for processing KICS/KATA version 3.x events.
Kaspersky Industrial CyberSecurity for Networks 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	The [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog normalizer is designed to process events received from the Kaspersky Industrial CyberSecurity for Networks 4.2 system via Syslog. This normalizer is deprecated. We recommend using the [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog normalizer.
Kaspersky Industrial CyberSecurity for Networks 4.2, 4.3, 4.5	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	Designed for processing events received from Kaspersky Industrial CyberSecurity for Networks (versions 4.2, 4.3, 4.5) via Syslog.
Kaspersky IoT Secure Gateway (KISG)	[OOTB] Kaspersky KISG syslog	Syslog	Designed for processing events received from Kaspersky IoT Secure Gateway (KISG) 3.0 via Syslog.
Kaspersky NGFW	[OOTB] Kaspersky NGFW CEF	cef	Designed for processing events received from the Kaspersky NGFW system version 1.0, 1.2 in CEF format.
Kaspersky NDR	[OOTB] Kaspersky NDR syslog	Syslog	Designed for processing events received from the Kaspersky NDR 7.0 system via Syslog. This package is available for KUMA version 3.2 or later.
Kaspersky Security Center	[OOTB] KSC	cef	Designed for processing Kaspersky Security Center events received in CEF format.
Kaspersky Security Center	[OOTB] KSC from SQL	sql	Designed for processing events received by the connector from the database of the Kaspersky Security Center system.
Kaspersky Security for Linux Mail Server (KLMS)	[OOTB] KLMS Syslog CEF	Syslog	Designed for processing events from Kaspersky Security for Linux Mail Server in CEF format via Syslog.
Kaspersky Security for MS Exchange SQL	[OOTB] Kaspersky Security for MS Exchange SQL	sql	Designed for processing Kaspersky Security for Exchange (KSE) 9.0 events stored in the database.
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG syslog CEF [OOTB] KSMG 2.1+ syslog CEF	Syslog	[OOTB] KSMG syslog CEF is a normalizer for processing KSMG 2.0 events received in CEF format via Syslog. [OOTB] KSMG 2.1+ syslog CEF is a normalizer for processing KSMG 2.1.1, 3.0 events received in CEF format via Syslog.
Kaspersky Unified Monitoring and Analysis Platform (KUMA)	[OOTB] KUMA forwarding	json	Designed to process events forwarded from Kaspersky Unified Monitoring and Analysis Platform (KUMA).
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF, [OOTB] KWTS (KV)	Syslog	The [OOTB] KWTS Syslog CEF normalizer is designed for processing events received from Kaspersky Web Traffic Security in CEF format via Syslog. The [OOTB] KWTS (KV) normalizer is designed for processing Kaspersky Web Traffic Security events in key-value format.
Keycloak	[OOTB] Keycloak syslog	Syslog	Designed for processing events of the Keycloak 26.3 system received via Syslog.

System name	Normalizer name	Type	Normalizer description
Kemp Technologies LoadMaster	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Kerio Control	[OOTB] Kerio Control	Syslog	Designed for processing events of Kerio Control firewalls.
LastLine Enterprise	[OOTB] LastLine Enterprise syslog cef	Syslog	Designed for processing events received from LastLine Enterprise 7.3, 8.1, 9.1 via Syslog in CEF format.
Libvirt	[OOTB] Libvirt syslog	Syslog	Designed for processing events of Libvirt version 8.0.0 received via Syslog.
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Linux	[OOTB] Linux audit and iptables Syslog v1	Syslog	Designed for processing events of the Linux operating system. This normalizer does not support processing events in the ENRICHED format.
Linux auditd	[OOTB] Linux auditd syslog for KUMA 3.2	Syslog	Designed for processing audit events (auditd package) of the Linux operating system received via Syslog. The normalizer supports events that have been processed by a KUMA collector version 3.2 or later.
Linux auditd	[OOTB] Linux auditd file for KUMA 3.2	regexp	Designed for processing audit events (auditd package) of the Linux operating system saved to a file. The normalizer supports events that have been processed by a KUMA collector version 3.2 or later.
MariaDB	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Designed for processing events coming from the MariaDB audit plugin over Syslog.
McAfee Endpoint DLP	[OOTB] McAfee Endpoint DLP syslog	Syslog	Designed for processing events received from McAfee Endpoint DLP Windows 11.10.200 via Syslog. This package is available for KUMA version 3.2 or later.
McAfee Web Gateway	[OOTB] McAfee Web Gateway	regexp	Designed for processing events from McAfee Web Gateway 7.8 and later in CEF and KV formats received via Syslog.
Microsoft Active Directory Certificate Services (AD CS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Active Directory Certificate Services (AD CS) log events in XML format. The [OOTB] Microsoft Products for KUMA 3 normalizer supports this event source in KUMA 3.0.1 and later versions.
Microsoft Active Directory Federation Service (AD FS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft AD FS events. The [OOTB] Microsoft Products for KUMA 3 normalizer supports this event source in KUMA 3.0.1 and later versions.
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft AD DS events. The [OOTB] Microsoft Products for KUMA 3 normalizer supports this event source in KUMA 3.0.1 and later versions.

System name	Normalizer name	Type	Normalizer description
Microsoft Defender	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Defender events.
Microsoft DHCP	[OOTB] MS DHCP file	regexp	Designed for processing Microsoft DHCP server events. The event source is Windows DHCP server logs.
Microsoft DNS	[OOTB] DNS Windows [OOTB] Microsoft DNS ETW logs json	regexp	The [OOTB] Windows DNS normalizer is designed to process Microsoft DNS server events. The event source is Windows DNS server logs. The normalizer does not support processing debug log events with the **Details** option enabled. The [OOTB] Microsoft DNS ETW logs json normalizer is designed to process some Microsoft DNS Server audit events supplied by the ETW provider. This package is available for KUMA version 3.2 or later.
Microsoft Exchange Server	[OOTB] Exchange CSV	csv	Designed for processing the event log of the Microsoft Exchange system. The event source is Exchange server MTA logs.
Microsoft Hyper-V	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Windows events. The event source is Microsoft Hyper-V logs: Microsoft-Windows-Hyper-V-VMMS-Admin, Microsoft-Windows-Hyper-V-Compute-Operational, Microsoft-Windows-Hyper-V-Hypervisor-Operational, Microsoft-Windows-Hyper-V-StorageVSP-Admin, Microsoft-Windows-Hyper-V-Hypervisor-Admin, Microsoft-Windows-Hyper-V-VMMS-Operational, Microsoft-Windows-Hyper-V-Compute-Admin.
Microsoft Installer	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Installer (MSI Installer) log events in XML format.
Microsoft IIS	[OOTB] IIS Log File Format	regexp	Designed for processing events from in the format described at https://learn.microsoft.com/en-us/windows/win32/http/iis-logging. The event source is Microsoft IIS logs.

System name	Normalizer name	Type	Normalizer description
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Windows events. The event source is Network Policy Server events.
Microsoft Office 365	[OOTB] Microsoft Office 365 json	json	Designed for processing Microsoft Office 365 audit events. This normalizer supports processing events received from Microsoft Teams, Azure Active Directory, SharePoint systems. This package is available for KUMA version 3.4 or later.
Microsoft SCCM	[OOTB] Microsoft SCCM file	regexp	Designed for processing events of the Microsoft SCCM system version 2309. This normalizer supports processing of some of the events stored in the AdminService.log file.
Microsoft SharePoint Server	[OOTB] Microsoft SharePoint Server diagnostic log file	regexp	Designed for processing some of Microsoft SharePoint Server 2016 events stored in diagnostic logs.
Microsoft Sysmon	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Sysmon module events.
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing part of events from the Security, System, Application logs of the Microsoft Windows operating system. The [OOTB] Microsoft Products via KES WIN normalizer supports a limited number of audit event types sent to KUMA by Kaspersky Endpoint Security 12.6 for Windows via Syslog.

System name	Normalizer name	Type	Normalizer description
Microsoft → Windows → AppLocker	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft → Windows → AppLocker log events in XML format.
Microsoft → Windows → DNS-Server → Audit	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft → Windows → DNS-Server → Audit log events in XML format.
Microsoft → Windows → Group Policy → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed to process Microsoft → Windows → Group Policy → Operational log events in XML format.
Microsoft → Windows → PowerShell	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Windows PowerShell log events.
Microsoft → Windows → PowerShell-Operational	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Windows PowerShell-Operational log events. The [OOTB] Microsoft Products via KES WIN normalizer supports a limited number of audit event types sent to KUMA by Kaspersky Endpoint Security 12.6 for Windows via Syslog.

System name	Normalizer name	Type	Normalizer description
Microsoft → Windows → System log → Netlogon	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft → Windows → System log → Netlogon log events in XML format.
Microsoft → Windows → TaskScheduler → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft → Windows → TaskScheduler → Operational log events in XML format.
Microsoft → Windows → WinRM → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft → Windows → WinRM → Operational log events in XML format.
Microsoft SQL Server	[Deprecated] [OOTB] Microsoft SQL Server xml	xml	Designed for processing events of MS SQL Server versions 2008, 2012, 2014, 2016. The normalizer supports KUMA 2.1.3 and later.
Microsoft SQL Server, Microsoft SQL Server Express	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed to process events of MS SQL Server 2008 or newer.
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing Microsoft Windows events. Event source → Applications and Services Logs → Microsoft → Windows → TerminalServices-LocalSessionManager → Operational log The "[OOTB] Microsoft Products via KES WIN" normalizer supports a limited number of audit event types sent to KUMA by Kaspersky Endpoint Security 12.6 for Windows via Syslog.

System name	Normalizer name	Type	Normalizer description
Microsoft Windows Service Control Manager	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing events from the Service Control Manager logs (System log) of the Microsoft Windows operating system.
Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing part of events from the Security, System logs of the Microsoft Windows Server operating system. The "[OOTB] Microsoft Products via KES WIN" normalizer supports a limited number of audit event types sent to KUMA by Kaspersky Endpoint Security 12.6 for Windows via Syslog.
Microsoft Windows XP/2003	[OOTB] SNMP. Windows {XP/2003}	json	Designed for processing events received from workstations and servers running Microsoft Windows XP, Microsoft Windows 2003 operating systems using the SNMP protocol.
Microsoft WSUS	[OOTB] Microsoft WSUS file	regexp	Designed for processing events of the Gardatech Perimeter system version 5.3, 5.4 received via Syslog.
MikroTik	[OOTB] MikroTik syslog	regexp	Designed for events received from MikroTik devices via Syslog.
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	Designed for processing events from the Minerva EDR system.
MongoDB	[OOTB] MongoDb syslog	Syslog	Designed for processing some events received from the MongoDB 7.0 database via Syslog.
Multifactor Radius Server for Windows	[OOTB] Multifactor Radius Server for Windows syslog	Syslog	Designed for processing events received from the Multifactor Radius Server 1.0.2 for Microsoft Windows via Syslog.
MySQL 5.7	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Designed for processing events coming from the MariaDB audit plugin over Syslog.
NetApp ONTAP (AFF, FAM)	[OOTB] NetApp syslog, [OOTB] NetApp file	regexp	[OOTB] NetApp syslog is a normalizer designed for processing events of the NetApp system (ONTAP 9.12 version) received via Syslog. [OOTB] NetApp file is a normalizer designed for processing events of the NetApp system (ONTAP 9.12 version) stored in a file.
NetApp SnapCenter	[OOTB] NetApp SnapCenter file	regexp	Designed to process part of the events of the NetApp SnapCenter system (SnapCenter Server 5.0). This normalizer supports processing some of the events from the C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\napManagerWeb.*.log file. Types of supported events in xml format from the SnapManagerWeb.*.log file: SmDiscoverPluginRequest, SmDiscoverPluginResponse, SmGetDomainsResponse, SmGetHostPluginStatusRequest, SmGetHostPluginStatusResponse, SmGetHostRequest, SmGetHostResponse, SmRequest. This normalizer supports processing some of the events from the C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\audit.log file.
Netgear Switch	[OOTB] Netgear Switch syslog	regexp	Designed for processing audit events from Netgear switches (model M4300-52G).

System name	Normalizer name	Type	Normalizer description
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
NetScout Systems nGenius Performance Manager	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Netwrix Endpoint Protector	[OOTB] Netwrix Endpoint Protector syslog	regexp	Designed for processing events received from the Netwrix Endpoint Protector 5.9 system via Syslog. This package is available for KUMA version 3.2 or later.
Nextcloud	[OOTB] Nextcloud syslog	Syslog	Designed for events of Nextcloud version 26.0.4 received via Syslog. The normalizer does not save information from the Trace field.
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
NFS kernel server	[OOTB] NFS kernel server syslog	regexp	Designed for processing NFS kernel server events (NFSv3, NFSv4.0, NFSv4.1, NFSv4.2) in Syslog format.
Nginx	[OOTB] nginx regexp	regexp	Designed for processing the event log of the nginx web server in the Combined format. The normalizer supports the processing of events received via Syslog and stored in a file. This package is available for KUMA version 3.2 or later.
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
NPO Fractel	[OOTB] NPO Fractel SSPT-4	regexp	Designed for processing events of the NPO Fractel SSPT-4A1 system.
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
OpenLDAP	[OOTB] OpenLDAP	regexp	Designed for line-by-line processing of some events of the OpenLDAP 2.5 system in an auditlog.ldif file.
OpenVPN	[OOTB] OpenVPN file	regexp	Designed for processing the event log of the OpenVPN system.
Oracle	[OOTB] Oracle Audit Trail	sql	Designed for processing database audit events received by the connector directly from an Oracle database.
Orion soft Cloudlink	[OOTB] OrionSoft Cloudlink syslog	regexp	Designed for processing events from the Orion soft Cloudlink 1.0 system in CEF format received via Syslog.
Orion soft Termit	[OOTB] OrionSoft Termit syslog	Syslog	Designed for processing events received from the Orion soft Termit 2.2, 2.3, 2.4 system via Syslog.
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	Designed for processing events of the Orion soft zVirt virtualization system (zVirt 3.1, 4.4, 4.5, 5.0 and zVirt Max 1.2).
PagerDuty	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Palo Alto Networks NGFW	[OOTB] Palo Alto NGFW syslog csv	Syslog	Designed for processing events from Palo Alto Networks firewalls received via Syslog in CSV format.
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Parsec ParsecNET	[OOTB] Parsec ParsecNET	sql	Designed for processing events received by the connector from the database of the Parsec ParsecNET 3 system.

System name	Normalizer name	Type	Normalizer description
Passwork	[OOTB] Passwork syslog	Syslog	Designed for processing events received from the Passwork version 050219 system via Syslog.
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	Designed for processing events from the PT Industrial Security Incident Manager system.
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PT NAD json	json	Designed for processing events coming from PT NAD in json format. This normalizer supports events from PT NAD version 11.1, 11.0.
Positive Technologies Multiscanner	[OOTB] PTsecurity Multiscanner json	Syslog	Designed for processing events from PT Multiscanner 5.24 in JSON format received via Syslog.
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	Designed for processing events of the PT Sandbox system.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF syslog	Syslog	Designed for processing events from PTsecurity Web Application Firewall 4 received via Syslog.
Postfix	[OOTB] Postfix syslog	regexp	Contains a resource set for processing Postfix 3.6 events. It supports processing Syslog events received over TCP. The package is available for KUMA 3.0 and newer versions.
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit Syslog	Syslog	Designed for processing events of the pgAudit audit plug-in for the PostgreSQL database received via Syslog.
PowerDNS	[OOTB] PowerDNS syslog	Syslog	Designed for processing events of PowerDNS Authoritative Server 4.5 received via Syslog.
Proftpd	[OOTB] Proftpd syslog	regexp	Designed for processing events received from Proftpd 1.3.8c via Syslog.
Proofpoint Insider Threat Management	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Proxmox	[OOTB] Proxmox file	regexp	Designed for processing events of the Proxmox system version 7.2-3 stored in a file. The normalizer supports processing of events in access and pveam logs.
PT NAD	[OOTB] PT NAD json	json	Designed for processing events coming from PT NAD in json format. This normalizer supports events from PT NAD version 11.1, 11.0.
QEMU - hypervisor logs	[OOTB] QEMU - Hypervisor file	regexp	Designed for processing events of the QEMU hypervisor stored in a file. QEMU 6.2.0 and Libvirt 8.0.0 are supported.
QEMU - virtual machine logs	[OOTB] QEMU - Virtual Machine file	regexp	Designed for processing events from logs of virtual machines of the QEMU hypervisor version 6.2.0, stored in a file.
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	Designed for processing events from the DDOS Mitigator protection system received via Syslog.
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider file	regexp	Designed for processing events of the Reak Soft Blitz Identity Provider system version 5.16, stored in a file.
RedCheck Desktop	[OOTB] RedCheck Desktop file	regexp	Designed for processing logs of the RedCheck Desktop 2.6 system stored in a file.
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	Designed for processing logs of the RedCheck Web 2.6 system stored in files.
RED SOFT RED ADM	[OOTB] RED SOFT RED ADM syslog	regexp	Designed for processing events received from the RED ADM system (RED ADM: Industrial edition 1.1) via Syslog. The normalizer supports processing: • Management subsystem events • Controller events

System name	Normalizer name	Type	Normalizer description
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	Designed for processing events from the pfSense firewall received via Syslog.
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	Designed for processing events from the pfSense firewall. The Syslog header of these events does not contain a hostname.
RuPost LLC WorksPad	[OOTB] RuPost LLC WorksPad CEF syslog	Syslog	Designed for processing part of the events of the RuPost LLC WorksPad system (version 6.3.70) in CEF format via Syslog.
SafeTech CA SQL	[OOTB] SafeTech CA SQL	sql	Designed to process events from the PostgreSQL DBMS of the SafeTech CA 3.2 system.
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
SaltStack	[OOTB] SaltStack syslog	Syslog	Designed for processing single-line events from the SaltStack system (version 3004.1 and later) received via Syslog. The normalizer does not support multi-line events.
SecurityCode Continent 3.9	[OOTB] SecurityCode Continent 3.9 json	json	Designed for processing SecurityCode Continent 3.9.2 events received from the kuma-kont utility in json format. This package is available for KUMA version 3.4 or later.
SecurityCode Continent 4	[OOTB] SecurityCode Continent 4 syslog	regexp	Designed for processing events of the SecurityCode Continent system version 4 received via Syslog.
Sendmail	[OOTB] Sendmail syslog	Syslog	Designed for processing events of Sendmail version 8.15.2 received via Syslog.
SentinelOne	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Seqrite EPS	[OOTB] Seqrite EPS CEF	cef	Designed for processing events from the Seqrite EPS 6.0 system in CEF format.
Skype for Business	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Designed for processing some of the events from the log of the Skype for Business system, the Lync Server log.
Snort	[OOTB] Snort 3 json file	json	Designed for processing events of Snort version 3 in JSON format.
Sophos Central	[OOTB] Sophos Central syslog	Syslog	Designed for processing some events received from Sophos Central 1.2 via Syslog in CEF format from the Sophos-Central-SIEM-Integration script.
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall syslog	Syslog	Designed to process events from the Sonicwall TZ firewall in key-value format (version 7.3), and in CEF format (versions 6.5, 7.3) received via Syslog.
Solar webProxy	[OOTB] Solar WebProxy syslog	regexp	Designed for processing events received from Solar webProxy 4.2 in siem-log format via Syslog.
SolarWinds DameWare MRC	[OOTB] SolarWinds DameWare MRC xml	xml	Designed for processing some of the DameWare Mini Remote Control (MRC) 7.5 events stored in the Application log of Windows. The normalizer processes events generated by the dwmrcs provider.
SolarWinds SFTP & SCP Server file	[OOTB] SolarWinds SFTP & SCP Server file	regexp	Designed for processing the SolarWinds SFTP & SCP Server 2.2 event log stored in the SftpServer.log file. This package is available for KUMA version 3.2 or later.

System name	Normalizer name	Type	Normalizer description
Sophos Firewall	[OOTB] Sophos Firewall syslog	regexp	Designed for processing events received from Sophos Firewall 20 via Syslog.
Sophos XG	[OOTB] Sophos XG	regexp	Designed for processing events from the Sophos XG firewall.
Squid	[OOTB] Squid access Syslog	Syslog	Designed for processing events of the Squid proxy server received via the Syslog protocol.
Squid	[OOTB] Squid access.log file	regexp	Designed for processing Squid log events from the Squid proxy server. The event source is access.log logs
Staffcop Enterprise	[OOTB] Staffcop Enterprise syslog CEF	regexp	Designed for processing events received from Staffcop Enterprise 5.4, 5.5 in CEF format via Syslog.
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	Designed for processing events from S-Terra VPN Gate devices.
Stormshield firewall	[OOTB] Stormshield firewall syslog	Syslog	Designed for processing events from Stormshield firewall 4.8 and 5.0 in key-value format via Syslog.
Suricata	[OOTB] Suricata json file	json	Designed for processing Suricata 7.0.1 events stored in a JSON file. This normalizer supports processing the following event types: flow, anomaly, alert, dns, http, ssl, tls, ftp, ftp_data, ftp, smb, rdp, pgsql, modbus, quic, dhcp, bittorrent_dht, rfb.
Synesis The Wall WAF	[OOTB] Synesis The Wall WAF syslog	Syslog	Designed for processing events of the Synesis TheWall WAF system received via Syslog.
TeamPass	[OOTB] TeamPass SQL	sql	Designed for processing events from the TeamPass 3.1 system stored in the database.
ThreatConnect Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Tionix Cloud Platform	[OOTB] Tionix Cloud Platform syslog	Syslog	Designed for processing events of the Tionix Cloud Platform system version 2.9 received via Syslog. The normalizer makes a partial selection of event data. The normalizer is available in KUMA 3.0 and later.
Tionix VDI	[OOTB] Tionix VDI file	regexp	Designed for processing some of the Tionix VDI system (version 2.8) events stored in the tionix_lntmov.log file.
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Trend Micro Control Manager	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Umbraco CMS	[OOTB] Umbraco CMS syslog	regexp	Designed for processing events of the Umbraco CMS version 11.4.1 in Syslog format.
Unbound	[OOTB] Unbound Syslog	Syslog	Designed for processing events from the Unbound DNS server received via Syslog.
UserGate	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format received from the UserGate system via Syslog.
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.

System name	Normalizer name	Type	Normalizer description
Veeam Software – Veeam Backup & Replication	[OOTB] Veeam Software Veeam Backup & Replication syslog	regexp	Designed for processing events from the Veeam Software – Veeam Backup & Replication 12.1 system via Syslog.
Veriato 360	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
ViPNet TIAS	[OOTB] ViPNet TIAS syslog	Syslog	Designed for processing events of ViPNet TIAS 3.8 received via Syslog.
VK Private Cloud	[OOTB] VK Private Cloud syslog	regexp	Designed for processing audit events of the VK Private Cloud 1.0 system received via Syslog.
VK WorkSpace Mail	[OOTB] VK WorkSpace Mail syslog	Syslog	Designed for processing events received from the VK WorkSpace Mail 1.23 system via Syslog in key-value format.
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	Designed for processing VMware ESXi events (support for a limited number of events from ESXi versions 5.5, 6.0, 6.5, 7.0) received via Syslog.
VMWare Horizon	[OOTB] VMware Horizon - Syslog	Syslog	Designed for processing events received from the VMware Horizon 2106 system via Syslog.
VMwareCarbon Black EDR	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Vmware Vcenter	[OOTB] VMware vCenter API	xml	Designed for processing VMware vCenter 7 events received via API.
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Vsftpd	[OOTB] Vsftpd syslog	regexp	Designed for processing events received from Vsftpd 3.0.5 via Syslog.
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	Designed for processing events received from the Wallix AdminBastion system via Syslog.
WatchGuard - Firebox	[OOTB] WatchGuard Firebox syslog	Syslog	Designed for processing WatchGuard Firebox (version OS v2026.1.B730198) events received via Syslog.
Webmonitorx	[OOTB] Webmonitorx json	regexp	Designed for processing events coming from the Webmonitorx system in JSON format. Also see the instructions on how to configure the receipt of Webmonitorx events in KUMA (the article is available only in Russian).
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Windchill FRACAS	[OOTB] PTC Winchill Fracas	regexp	Designed for processing events of the Windchill FRACAS failure registration system.
Yandex Cloud	[OOTB] Yandex Cloud	regexp	Designed for processing a part of Yandex Cloud audit events. This normalizer supports processing audit log events of the configuration level: IAM (Yandex Identity and Access Management), Compute (Yandex Compute Cloud), Network (Yandex Virtual Private Cloud), Storage (Yandex Object Storage), Resourcemanager (Yandex Resource Manager), Backup.
Zabbix	[OOTB] Zabbix SQL	sql	Designed for processing events of Zabbix 6.4.
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	Designed to process a part of events of the Zecurion DLP system version 13.0 received in CEF format via Syslog.
ZEEK IDS	[OOTB] ZEEK IDS json file	json	Designed for processing logs of the ZEEK IDS system in JSON format. The normalizer supports events from ZEEK IDS version 1.8.
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format.

System name	Normalizer name	Type	Normalizer description
IT-Bastion – Synonyx	[OOTB] Bastion Synonyx CEF	regexp	Designed for processing events in the CEF format received from the IT-Bastion Synonyx 1.7 system. This normalizer package is available for KUMA version 3.2 or later.
IT-Bastion – SKDPU	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format received from the IT-Bastion SKDPU system via Syslog.
A-Real Internet Control Server (ICS)	[OOTB] A-real IKS syslog	regexp	Designed for processing events of the A-Real Internet Control Server (ICS) system received via Syslog. The normalizer supports events from A-Real ICS version 7.0 and later.
Biznes Resheniya Compass	[OOTB] Biznes Resheniya Compass	regexp	Designed for processing audit event types of Biznes Resheniya Compass 6.7.7 and 6.7.8 received via Kafka.
Angie web server	[OOTB] Angie syslog	Syslog	Designed for processing events received from Angie and Angie Pro (version 1.10.1) via Syslog. This normalizer package is available for KUMA version 3.2 or later.
Apache web server	[OOTB] Apache HTTP Server file	regexp	Designed for processing Apache HTTP Server 2.4 events stored in a file. The normalizer supports processing of events from the Application log in the Common or Combined Log formats, as well as the Error log. Expected format of the Error log events: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Apache web server	[OOTB] Apache HTTP Server syslog	Syslog	Designed for processing events of the Apache HTTP Server received via Syslog. The normalizer supports processing of Apache HTTP Server 2.4 events from the Access log in the Common or Combined Log format, as well as the Error log. Expected format of the Error log events: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Lighttpd web server	[OOTB] Lighttpd syslog	Syslog	Designed for processing Access events of the Lighttpd system received via Syslog. The normalizer supports processing of Lighttpd version 1.4 events. Expected format of Access log events: `$remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"`
IVK Kolchuga-K	[OOTB] Kolchuga-K Syslog	Syslog	Designed for processing events from the IVK Kolchuga-K system, version LKNV.466217.002, via Syslog.
InfoTeCS ViPNet IDS	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format received from the InfoTeCS ViPNet IDS system via Syslog.
InfoTeCS ViPNet Coordinator	[OOTB] ViPNet Coordinator Syslog [OOTB] ViPNet Coordinator CEF	Syslog	The [OOTB] ViPNet Coordinator Syslog normalizer is designed to process events from the InfoTeCS ViPNet Coordinator system via Syslog. The [OOTB] ViPNet Coordinator CEF normalizer is designed to process events received from the InfoTeCS ViPNet Coordinator (version 4.5) in CEF format.
Kod Bezopasnosti —Continent	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	Designed for processing events of Continent IPS/IDS device log.
Kod Bezopasnosti —Continent	[OOTB] Continent SQL	sql	Designed for getting events of the Continent system from the database.
Kod Bezopasnosti SecretNet 7	[OOTB] SecretNet SQL	sql	Designed for processing events received by the connector from the database of the SecretNet system.
Confident – Dallas Lock Unified Control Center	[OOTB] Confident Dallas Lock syslog CEF	regexp	Designed to process events from systems: Dallas Lock 8 (version 11.4.2.843, 12.10.6.877), Dallas Lock Unified Control Center (ECU) (version 4.0.294.0, 4.0.354.0) in CEF format.
Confident - Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Designed for processing events received from Dallas Lock 8 (version 11.4.2) in CEF format.
CryptoPro NGate	[OOTB] Ngate Syslog	Syslog	Designed for processing events received from the CryptoPro NGate system via Syslog.
H3C (Huawei-3Com) routers	[OOTB] H3C Routers syslog	regexp	Designed for processing events received from H3C (Huawei-3Com) SR6600 network devices (Comware 7 firmware) via Syslog. The normalizer supports the "standard" event format (RFC 3164-compliant format).

System name	Normalizer name	Type	Normalizer description
NT Monitoring and Analytics	[OOTB] Syslog-CEF	Syslog	Designed for processing events in the CEF format received from the NT Monitoring and Analytics system via Syslog.
BlueCoat proxy server	[OOTB] BlueCoat Proxy v0.2	regexp	Designed to process BlueCoat proxy server events. The event source is the BlueCoat proxy server event log.
SKDPU NT Access Gateway	[OOTB] Bastion SKDPU-GW syslog	Syslog	Normalizer for processing system events of the SKDPU NT Access gateway 7.0 (build 17, update 14) and 7.1.1 received via Syslog.
Solar Dozor	[OOTB] Solar Dozor Syslog	Syslog	Designed for processing events received from the Solar Dozor system version 7.9 via Syslog. The normalizer supports custom format events and does not support CEF format events.
Yandex 360	[OOTB] Yandex 360 json	json	Designed for processing events received from the Yandex 360 system in JSON format. The transport for receiving events will be available in KUMA 4.2.
Yandex Browser corporate	[OOTB] Yandex Browser	json	Designed for processing events received from the corporate version of Yandex Browser 23, 24.4, 25.2.
-	[OOTB] Syslog header	Syslog	Designed for processing events received via Syslog. The normalizer parses the header of the Syslog event, the message field of the event is not parsed. If necessary, you can parse the message field using other normalizers.

Creating a collector

You can create a collector in the Kaspersky SIEM web interface in one of the following ways:

- In the **Resources** section, click **Connect source**.
- Under **Resources** → **Collectors**, click **New**.

The collector is created using the following steps:

1 Connect event sources

1. On the **Basic settings** tab, under **Connect event sources**, fill in the following fields:

   a. In the **Collector name** field, enter a unique name for the collector. The name must contain 1 to 128 Unicode characters.

   When certain types of collectors are created, agents named `agent: <Collector name>, auto created` are also automatically created together with the collectors. If this type of agent was previously created and has not been deleted, it will be impossible to create a collector named `<Collector name>`. In this case you will have to either specify a different name for the collector or delete the previously created agent.

   b. In the **Tenant** drop-down list, select the tenant that you want to own the collector. The tenant selection determines what resources will be available when the collector is created.

   > If, when creating a collector, you return to the **Connect event sources** section and select a different tenant, you must manually update all resources that you added to the service. Only resources from the selected tenant and the Shared tenant can be added to the service.

c. If necessary, in the **Handlers** field, specify the number of handlers that the collector can run simultaneously to process events in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.

d. You can use up to 256 Unicode characters to describe the collector in the **Description** field.

2. On the **Advanced settings** tab, fill in the following fields:

   a. If necessary, use the **Debug** toggle switch to enable logging of service operations. Error messages of the collector service are logged even when debug mode is disabled. You can view the log on the computer where the collector is installed, in the `/opt/kaspersky/kuma/collector/<collector ID>/log/collector` directory.

   b. You can use the **Create dump periodically** toggle switch at the request of Technical Support to generate resource (for example, CPU, RAM) utilization reports in the form of dumps.

   c. In the **Dump settings** field, you can specify the settings to be used when creating dumps. For instructions on filling out this field, please contact Technical Support.

2 Adding a connector

1. On the **Basic settings** tab, under **Transport**, in the **Connector** drop-down list, select the required connector or create a new one by clicking **New**.

   If you select a connector from the list, the **Transport** section displays the settings of the selected connector.

2. If you clicked **Create**, in the **Type** drop-down list, select the connector type and specify its settings under **Basic settings** and **Advanced settings** tabs. The available settings depend on the selected type of connector:

   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - 1c-log
   - 1c-xml

- diode
- ftp
- nfs
- wmi
- wec
- etw
- snmp
- snmp-trap
- kata\edr
- vmware
- elastic
- office365
- dfi
- universalAPI
- smb

When using the **tcp** or **udp** connector type at the normalizer addition stage, IP addresses of the devices from which the events were received will be written in the `DeviceAddress` event field (if it is empty).

When using a **wmi**, **wec**, or **etw** connector, agents are automatically created for receiving Windows events.

It is recommended to use the default encoding (UTF-8), and to apply other settings only if bit characters are received in the fields of events.

Making KUMA collectors to listen on ports up to `1,000` requires running the service of the relevant collector with root privileges. To do this, after installing the collector, add the following string to the `systemd` configuration file in the `[Service]` section:

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

The systemd file is located in the `/usr/lib/systemd/system/kuma-collector-<collector ID>.service directory`.

The connector is added to the resource set of the collector. The created connector is only available in this resource set and is not displayed in the web interface **Resources** → **Connectors section**.

3 Adding a normalizer

1. In the **Event parsing** section, in the **Parsing scheme** tab, click **+ Add event parsing**.

2. If you want to create the normalizer as a separate resource, select the **Save normalizer** check box. If the check box is selected, the normalizer becomes available for selection in other collectors of the tenant. This check box is cleared by default.

3. In the **Name** field, enter a unique name for the normalizer. Maximum length of the name: 128 Unicode characters.

   a. In the **Parsing method** drop-down list, select the type of events to receive. Depending on the selected value, you can use the predefined event field matching rules or define rules manually. When you select some parsing methods, additional settings may become available that you must specify.

   Available parsing methods:

   json

   This parsing method is used to process JSON data where each object, including its nested objects, occupies a single line in a file.

   When processing files with hierarchically structured data, you can reference the fields of nested objects using the dot notation. For example, the `username` parameter from the string `"user": {"username": "system: node: example-01"}` can be accessed by using the `user.username` query.

   Files are processed line by line. Multi-line objects with nested structures may be normalized incorrectly.

   In complex normalization schemes where additional normalizers are used, all nested objects are processed at the first normalization level, except for cases when the extra normalization conditions are not specified and, therefore, the event being processed is passed to the extra normalizer in its entirety.

   You can use `\n` and `\r\n` as newline characters. Strings must be UTF-8 encoded.

   If you want to send the raw event for advanced normalization, at each nesting level in the **Advanced event parsing** window, in the **Use raw event** drop-down list, select **Yes**.

   cef

   This parsing method is used to process CEF data.

   If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**.

   regexp

   This parsing method is used to create custom rules for processing data in a format using regular expressions.

   You must add a regular expression (RE2 syntax) with named capturing groups to the field under **Normalization**. The name of the capturing group and its value are considered the field and value of the raw event that can be converted to an event field in KUMA format.

To add event handling rules:

1. If necessary, copy an example of the data you want to process to the **Event examples** field. We recommend completing this step.

   You can also generate regular expressions based on added examples by clicking the **Generate regular expression with KIRA** button. This automatically adds generated regular expressions to the **Normalization** group of settings.

2. In the field under **Normalization**, add a regular expression with named capture groups following the RE2 syntax, for example `"(?P<name>regexp)"`. The regular expression added to the field under **Normalization** must exactly match the event. When designing the regular expression, we recommend using special characters that match the starting and ending positions of the text: `^`, `$`.

   You can add multiple regular expressions or remove regular expressions. To add a regular expression, click **Add regular expression**. To remove a regular expression, click the delete icon ✕ next to it.

3. Click the **Copy field names to the mapping table** button.

   Capture group names are displayed in the **KUMA field** column of the **Mapping** table. You can select the corresponding KUMA field in the column opposite each capturing group. If you followed the CEF format when naming the capturing groups, you can use automatic CEF mapping by selecting the **Use CEF syntax for normalization** check box.

Event handling rules are added.

syslog

This parsing method is used to process data in syslog format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**.

To parse events in rfc5424 format with a `structured-data` section, in the **Keep extra fields** drop-down list, select **Yes**. This makes the values from the `structured-data` section available in the `Extra` fields.

csv

This parsing method is used to create custom rules for processing CSV data.

When choosing this parsing method, you must specify the separator of values in the string in the **Delimiter** field. Any single-byte ASCII character can be used as a delimiter for values in a string.

kv

This parsing method is used to process data in key-value pair format. Available parsing method settings are listed in the table below.

Available parsing method settings

Setting	Description
Pair delimiter	The character used to separate key-value pairs. You can specify any single-character (1 byte) value. The specified value must not match the value specified in the **Value delimiter** field.
Value delimiter	The character used to separate a key from its value. You can specify any single-character (1 byte) value. The specified value must not match the value specified in the **Pair delimiter** field.

xml

This parsing method is used to process XML data in which each object, including nested objects, occupies a single line in a file. Files are processed line by line.

If you want to send the raw event for advanced normalization, at each nesting level in the **Advanced event parsing** window, in the **Use raw event** drop-down list, select **Yes**.

If you select this parsing method, under **XML attributes**, you can specify the key XML attributes to be extracted from tags. If an XML structure has multiple XML attributes with different values in the same tag, you can identify the necessary value by specifying the key of the value in the **Source** column of the **Mapping** table.

To add key XML attributes:

1. Click **+ Add field**.

2. This opens a window; in that window, specify the path to the XML attribute.

You can add multiple XML attributes or remove XML attributes. To remove an individual XML attribute, click the delete icon ✕ next to it. To remove all XML attributes, click **Reset**.

If XML key attributes are not specified, then in the course of field mapping the unique path to the XML value will be represented by a sequence of tags.

Tag numbering

Starting with KUMA 2.1.3, you can use automatic tag numbering in XML events. This lets you parse an event with the identical tags or unnamed tags, such as `<Data>`.

As an example, we will number the tags of the `EventData` attribute of the Microsoft Windows PowerShell event ID 800.

View Microsoft Windows PowerShell events, event ID 800

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
        <System>
                <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-
8497-1e730c959516}" EventSourceName="NTDS" />
                <EventID Qualifiers="0000">0000</EventID>
                <Version>@</Version>
                <Level>4</Level>
                <Task>15</Task>
                <Opcode>0</Opcode>
                <Keywords >0x8080000000000000</Keywords>
                <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
                <EventRecordID>55647</EventRecordID>
                <Correlation />
                <Execution ProcessID="1" ThreadID="1" />
                <Channel>service</Channel>
                <Computer>computer</Computer>
                <Security UserID="0000" />
        </System>
        <EventData>
                <Data>583</Data>
                <Data>36</Data>
                <Data>192.168.0.1:5084</Data>
                <Data>level</Data>
                <Data>name, lDAPDisplayName</Data>
                <Data />
                <Data>5545</Data>
                <Data>3</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>15</Data>
                <Data>none</Data>
```

```
        </EventData>
</Event>
```

To parse events with identical tags or unnamed tags, you need to configure tag numbering and data mapping for numbered tags with KUMA event fields.

KUMA 3.0.x supports using XML attributes and tag numbering at the same time in the same extra normalizer. If an XML attribute contains unnamed tags or identical tags, we recommend using tag numbering. If the XML attribute contains only named tags, we recommend using XML attributes.

To use XML attributes and tag numbering in extra normalizers, you must sequentially enable the **Use raw event** setting in each extra normalizer along the path that the event follows to the target extra normalizer, and in the target extra normalizer itself.

For an example of how tag numbering works, you can refer to the **MicrosoftProducts** normalizer. The **Use raw event** setting is enabled sequentially in both **AD FS** and **424** extra normalizers.

To set up the parsing of events with unnamed or identical tags:

1. Open an existing normalizer or create a new normalizer.

2. In the **Basic event parsing** window of the normalizer, in the **Parsing method** drop-down list, select **xml**.

3. In the **Tag numbering** field, click **+ Add field**.

4. In the displayed field, enter the full path to the tag to whose elements you want to assign a number, for example, `Event.EventData.Data`. The first tag gets number 0. If the tag is empty, for example, `<Data />`, it is also assigned a number.

5. To configure data mapping, under **Mapping**, click **+ Add row** and do the following:

   a. In the displayed row, in the **Source** field, enter the full path to the tag and the index of the tag. For example, for the Microsoft Windows PowerShell event ID 800 from the example above, the full paths to tags and tag indices are as follows:

      - `Event.EventData.Data.0`
      - `Event.EventData.Data.1`
      - `Event.EventData.Data.2`

   b. In the **KUMA field** drop-down list, select the field in the KUMA event that will receive the value from the numbered tag after parsing.

6. Save changes in one of the following ways:

   - If you created a new normalizer, click **Save**.
   - If you edited an existing normalizer, in the collector to which the normalizer is linked, click **Update configuration**.

Parsing is configured.

netflow

This parsing method is used to process data in all supported NetFlow protocol formats: NetFlow v5, NetFlow v9, and IPFIX.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. This takes into account the source fields of all NetFlow versions (NetFlow v5, NetFlow v9, and IPFIX).

If the **netflow** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

netflow5

This parsing method is used to process data in the NetFlow v5 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **netflow5** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow5** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

netflow9

This parsing method is used to process data in the NetFlow v9 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **netflow9** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow9** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

sflow5

This parsing method is used to process data in sflow5 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **sflow5** parsing method is selected for the main parsing, extra normalization is not available.

ipfix

This parsing method is used to process IPFIX data.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **ipfix** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **ipfix** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

sql

The normalizer uses this parsing method to process data obtained by making a selection from the database.

This parsing method becomes available only if you added the sql type connector in the "Transport" section.

normalizer

This parsing method allows you to reuse a previously created normalizer as the primary or extra normalizer for processing events.

If you select this parsing method, in the **Normalizer** drop-down list, you need to select one of the previously created normalizers of the json, cef, regexp, syslog, csv, kv, xml, or sql type. Normalizers with the **normalizer** parsing method cannot be selected.

b. In the **Keep raw event** drop-down list, specify whether you want to store the original raw event in the re-created normalized event.

- **Don't save**—do not save the raw event. This value is selected by default.
- **Only errors**—save the raw event in the `Raw` field of the normalized event if errors occurred when parsing it. You can use this value to debug the service. In this case, an event having a non-empty `Raw` field will indicate problems.
- **Always**—always save the raw event in the `Raw` field of the normalized event.

c. In the **Keep extra fields** drop-down list, choose whether you want to store the raw event fields in the normalized event if no mapping has been configured for them.

This field is not available if the **Parsing method** is set to **normalizer**.

- **No**. This value is selected by default.
- **Yes**. The original event fields are saved in the `Extra` field of the normalized event.

d. If necessary, provide an example of the data you want to process to the **Event examples** field. We recommend completing this step.

This field is not available if the **Parsing method** is set to **normalizer**.

You can add multiple event examples. Every new example must be specified on a new line. At the same time, in the **Mapping** table, its parsing result will be displayed in the **Examples** column. This lets you check whether the fields of different types of incoming events are mapped correctly.

Limitations involved in parsing event examples

When parsing the examples of data specified in the **Event examples** field, the following parameters are not taken into account in the extra normalizer:

- Enrichment configured in the root normalizer
- Filters specified in the extra normalizer
- The **Use raw event** setting
- Conversions in the root normalizer
- Conversions for the value of the **Field to pass into normalizer** parameter.

4. In the **Mapping** settings block, configure the mapping of raw event fields to KUMA event fields:

   a. Click **+ Add row**.

   You can add multiple table rows or delete table rows. To delete a table row, select the check box next to it and click the **Delete** button.

   b. In the **Source** column, specify the name of the raw event field that you want to map to the KUMA event field.

   For details about the field name format, refer to the Normalized event data model article. For a description of the mapping, refer to the Mapping fields of predefined normalizers article.

   If you want to create rules for modifying the fields of the original event before writing to the KUMA event fields, click the settings (⚙) icon next to the field name to open the **Conversion** window, and in that window, click **+ Add conversion**. You can reorder the rules or delete the rules. To reorder rules, use the reorder (⠿) icons. To delete a rule, click the delete (✕) icon next to it.

   Available conversions

   Conversions are modifications that are applied to a value before it is written to the event field.

   You can select one of the following conversion types from the drop-down list:

   - **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

   - **lower**—is used to make all characters of the value lowercase

   - **upper**—is used to make all characters of the value uppercase

   - **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

   - **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

   - **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

     - **Replace chars** specifies the sequence of characters to be replaced.

     - **With chars** is the character sequence to be used instead of the character sequence being replaced.

   - **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

   - **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

   - **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:
  - **Expression** is the RE2 regular expression whose results you want to replace.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.
- Converting encoded strings to text:
  - **decodeHexString**—used to convert a HEX string to text.
  - **decodeBase64String**—used to convert a Base64 string to text.
  - **decodeBase64URLString**—used to convert a Base64url string to text.
  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.
- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.
- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

If in the **Transport** section you specified the file type connector, you can pass the name or path of the file being processed by the collector to the KUMA event field. To do this, in the **Source** column, specify one of the following values:

```
Pass the name of the file processed by the collector in the KUMA event field
```

```
$kuma_fileSourceName
```

```
Pass the path to the file processed by the collector in the KUMA event field
```

```
$kuma_fileSourcePath
```

When you use a **file** connector, the new variables in the normalizer will only work with destinations of the internal type.

c. In the **KUMA field** column, select a KUMA event field from the drop-down list. You can find the KUMA event field by typing its name. If the name of the KUMA event field begins with `DeviceCustom*` or `Flex*`, enter a unique custom label in the **Label** field, if necessary.

If you want KUMA to enrich events with asset information, and the asset information to be available in the alert card when a correlation rule is triggered, in the **Mapping** table, configure a mapping of host address and host name fields depending on the purpose of the asset. For example, you can configure a mapping for **SourceAddress** and **SourceHostName**, or **DestinationAddress** and **DestinationHostName** KUMA event fields. As a result of enrichment, the event card includes a **SourceAssetID** or **DestinationAssetID** KUMA event field, and a link to the asset card. As a result of enrichment, asset information is also available in the alert card.

If you have loaded data into the **Event examples** field, the table will have an **Examples** column containing examples of values carried over from the raw event field to the KUMA event field.

The **Mapping** table is not available if the **Parsing method** is set to **normalizer**.

5. To add data to the created normalized events, create enrichment rules in the normalizer as follows:

a. Go the **Enrichment** tab.

The **Enrichment** tab is not available if on the **Normalization scheme** tab, the **Parsing method** is set to **normalizer**.

b. Click the **+ Add enrichment** button.

The enrichment rule settings section is displayed. You can add multiple enrichment rules or delete enrichment rules. To delete an enrichment rule, click the delete (×) icon next to it.

c. In the **Source kind** drop-down list, select the type of the enrichment source. When you select some enrichment source types, additional settings may become available that you must specify.

Available Enrichment rule source types:

constant

This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "constant"

Setting	Description
Constant	The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed.
Target field	The event field to insert the data into.

If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field.

If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array.

dictionary

This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dictionary"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.

If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`.

If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`.

table

This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "table"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.
Mapping	Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`).

The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field.

If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

event

This type of enrichment is used when you need to write a value from another event field to the current event field. Available enrichment type settings are listed in the table below.

Available enrichment type settings

Setting	Description
Target field	The KUMA event field that you want to populate with the data.
Source field	The event field whose value is written to the target field.

If you want to create a rule for modifying the raw data before writing to KUMA event fields, under **Conversion**, click the **+ Add conversion** button. In the **Type** drop-down list, select a conversion type. You can add multiple conversion by clicking the **+ Add conversion** button. To delete an added conversion, click the trashcan icon next to it.

Available conversions

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

- **lower**—is used to make all characters of the value lowercase

- **upper**—is used to make all characters of the value uppercase

- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:

  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.

  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

When using enrichment of events that have **event**selected as the **Source kind** and the extended event schema fields are used as arguments, the following special considerations apply:

- If the source extended event schema field has the `Array of strings` type, and the target extended event schema field has the `String` type, the values are written to the target extended event schema field in TSV format.

  Example: the `SA.StringArray` extended event schema field contains values: `"string1"`, `"string2"`, `"string3"`. An event enrichment operation is performed. The result of the event enrichment operation is written to the `DeviceCustomString1` extended event schema field. The `DeviceCustomString1` extended event schema field contains values: `["string1", "string2", "string3"]`.

- If the source and target extended event schema fields have the `Array of strings` type, values of the source extended event schema field are added to the values of the target extended event schema field, and the `","` character is used as the delimiter.

  Example: The `SA.StringArrayOne` field of the extended event scheme contains the `["string1", "string2", "string3"]` values, and the `SA.StringArrayTwo` field of the extended event scheme contains the `["string4", "string5", "string6"]` values. An event enrichment operation is performed. The result of the event enrichment operation is written to the `SA.StringArrayTwo` field of the extended event scheme. The `SA.StringArrayTwo` extended event schema field contains values: `["string4", "string5", "string6", "string1", "string2", "string3"]`.

template

This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

dns

This type of enrichment is used to send requests to a private network DNS server to convert IP addresses into domain names or vice versa. IP addresses are converted to DNS names only for private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dns"

Setting	Description
URL	URL of the DNS server to which you want to send requests. You can use the **Add URL** button to specify multiple URLs. If the **URL** setting is not specified, KUMA takes the list of DNS servers from the localhost's `/etc/resolv.conf` file. In this case, you need to enable the **Recursive queries** option. Otherwise, the enrichment will not occur.
Requests per second	Maximum number of queries sent to the DNS server per second. By default, this value is equal to the number of vCPUs of the KUMA Core server.

Setting	Description
Workers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used. The default value is `1`.
Maximum number of events in enrichment queue	The maximum number of events to hold in the resubmission queue. The default value is `1,000,000`.
Timeout	The time to wait for a response from the DNS server (in seconds). The default value is `5`.
DNS mode override	Resolution method used: • **Forward DNS only** resolves a domain name to an IP address. • **Reverse DNS only** resolves an IP address to a domain name. • **Forward and reverse DNS** resolves a domain name to an IP address or an IP address to a domain name.
Cache TTL	The lifetime (in seconds) of values stored in the cache. The default value is `60` seconds.
Cache disabled	You can enable or disable caching using this setting. Caching is enabled by default.
Cache refresh disabled	If cache update is enabled, then upon expiry of the cache's TTL the collector sends repeated requests to the DNS server to update the data stored in the cache. This setting is available only when cache is enabled. By default, cache update is enabled.
Recursive queries	Allows a collector to send recursive queries to authoritative DNS servers for the purposes of enrichment. The default value is **Disabled**.

cybertrace

For systems with high load on a collector or correlator, we recommend using the **cybertrace-http** enrichment type. This type of enrichment returns a structured JSON response and correctly distinguishes between strings and arrays of custom attributes, preventing parsing errors.
When **cybertrace** enrichment is used, the collector receives an unstructured response. If the value of a custom attribute in Kaspersky CyberTrace contains square brackets, for example, **[str1**, **str2]**, Kaspersky SIEM treats it as an array, not a string.

This type of enrichment is used to add information from Kaspersky CyberTrace data feeds to event fields. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace"

Setting	Description
URL	URL of the Kaspersky CyberTrace server which you want to send requests to. The default Kaspersky CyberTrace port is 9999. Required setting.
Number of connections	Maximum number of connections to the Kaspersky CyberTrace server that can be established simultaneously by Kaspersky SIEM. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Requests per second	Maximum number of requests sent to the server per second. The default value is `1000`.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`.
Mapping	Table for mapping event fields to the types of indicators in Kaspersky CyberTrace. The **KUMA field** column shows the names of event fields, and the **CyberTrace indicator** column shows the types of Kaspersky CyberTrace indicators. Available types of Kaspersky CyberTrace indicators: • **ip** • **url** • **hash**

In the mapping table, you must provide at least one string. You can add new table rows or delete table rows. To add a new table row, click **Add row**. To delete a row in the table, click the ✕ cross.

cybertrace-http

This streaming event enrichment type in Kaspersky CyberTrace allows you to send a large number of events to the CyberTrace API-interface with a single request. We recommend using the **cybertrace-http** enrichment type for systems with a large stream of events. The **cybertrace-http** enrichment type performs better than the **cybertrace** enrichment type.

Limitations:

- The **cybertrace-http** enrichment type cannot be used for retrospective scanning in KUMA.
- When the **cybertrace-http** enrichment type is used, cyberthreat detections are not saved in Kaspersky CyberTrace history in the **Detections** window.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace-http"

Setting	Description
Tenant	Tenant, within which you plan to work with Kaspersky CyberTrace. Required setting.
URL	URL of the Kaspersky CyberTrace server to which you want to send requests, and the port used by the CyberTrace API. The default port is 443. Required setting.
Secret	The drop-down list where you can select the secret that stores the connection credentials. Required setting.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Key fields	The list of event fields used for enriching events with data from Kaspersky CyberTrace. Required setting.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`. After reaching 1 million events received from the Kaspersky CyberTrace server, events stop being enriched until the number of received events is reduced to less than 500,000.
CyberTrace main version	Kaspersky CyberTrace version. Available values: • **<5**—requests are executed in the General tenant in Kaspersky CyberTrace, and use the new API version provided by Kaspersky CyberTrace 5.0 and later. • **≥ 5.0**—requests use the API version that corresponds to Kaspersky CyberTrace 4.x. The default value is **<5**.
Debug	The parameter that enables resource logging. The toggle switch is turned off by default.
Tags	Tags for resource search.

timezone

This type of enrichment is used in collectors and correlators to assign a specific time zone to an event. Time zone information may be useful when searching for events that occurred at unusual times, such as nighttime.

When this type of enrichment is selected, the required time zone must be selected from the **Time zone** drop-down list.

> Make sure that the selected time zone is set on the server hosting the enrichment-utilizing service. For example, you can do this by using the `timedatectl list-timezones` command, which shows all time zones that are set on the server. For more details on setting time zones, please refer to your operating system documentation.

When an event is enriched, the time offset of the selected time zone relative to Coordinated Universal Time (UTC) is written to the DeviceTimeZone event field in the `+-hh:mm` format. For example, if you select the **Asia/Yekaterinburg** time zone, the value `+05:00` will be written to the `DeviceTimeZone` field. If an enriched event already has a value in the `DeviceTimeZone` field, it will be overwritten.

By default, if the timezone is not specified in the event being processed and enrichment rules by timezone are not configured, the event is assigned the timezone of the server hosting the service (collector or correlator) that processes the event. If server time is changed, the service must be restarted.

Permissible time formats when enriching the DeviceTimeZone field

When processing incoming raw events in the collector, the following time formats can be automatically converted to the `+-hh:mm` format (see the table below):

Time format in a processed event	Example
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

If the date format in the `DeviceTimeZone` field differs from those listed in the table, the collector server time zone is written to the field when an event is enriched with time zone information. You can create normalization rules for non-standard time formats.

geographic data

This type of enrichment is used to add IP address geographic data to event fields.

When this type is selected under **Mapping geographic data to event fields** parameter block, you need to specify from which event field the IP address will be read, select the attributes of geographic data, and define the event fields to which geographic data will be written:

1. In the **Event field with IP address** drop-down list, select the event field from which the IP address is read. Geographic data uploaded to KUMA is matched against this IP address.

   > When the `SourceAddress`, `DestinationAddress`, and `DeviceAddress` event fields are selected, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields.

2. For each event field you need to read the IP address from, select the type of geographic data and the event field to which the geographic data should be written.

   - In the **Geodata attribute** field, select which geographic data corresponding to the read IP address should be written to the event. Available geographic data attributes: **Country**, **Region**, **City**, **Longitude**, **Latitude**.

   - In the **Event field to write to**, select the event field which the selected geographic data attribute must be written to.

   You can use the **Add geodata attribute** button to add field pairs for **Geodata attribute** – **Event field to write to**. You can also configure different types of geographic data for one IP address to be written to different event fields.

3. To add each subsequent mapping, click the **Add mapping** button and repeat the previous two steps of these instructions.

   You can write identical geographic data attributes to different event fields. If you configure multiple geographic data attributes to be written to the same event field, the event will be enriched with the last mapping in the sequence.

check DLL Hijacking

DLL Hijacking is an attack technique that involves delivering vulnerable legitimate software along with a malicious dynamic link library (DLL) to a target system. To detect such attacks, Kaspersky SIEM uses the AI module. The AI module analyzes the launch and runtime parameters of applications and identifies suspicious launches of legitimate software with malicious libraries.

To get a status, Kaspersky SIEM sends a request with information from event fields to <KSN>. In response to the request, KSN sends the analysis result.

You can configure DLL Hijacking attack detection in the collector or correlator.

> To use enrichment such as **check DLL Hijacking**, your license must include the AI module. The General administrator needs also to accept the additional KSN Statement in the **Kaspersky Security Network** section (**Settings** → **Integrations** → **AI services** → **DLL Hijacking detection**).

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "DLL Hijacking"

Setting	Description
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.
Maximum cache size	Maximum cache size for KSN responses, in megabytes. The default value is `128 MB`. Each KSN response has its own lifetime, during which it is retained in the cache. If Kaspersky SIEM sends a second request for a DLL file for which KSN has already issued a response, and the lifetime of that response has not yet expired, the request is not actually sent to KSN, but the response is taken from the cache.
Maximum number of events in enrichment queue	If the specified value is exceeded, new events are not processed. The default value is `1,000,000`. `0` means that event processing stops if the queue contains any number of events.

Perform a repeat request	KSN response may return the **Unclassified** status. This status means that KSN has accepted the request and is currently processing it, but there is no status yet. Processing may take a long time, so the request must be re-sent.
	If this setting is enabled, specify additional settings:
	• If the **Create duplicates** setting is enabled, KUMA creates a duplicate event and uses it for repeated requests to KSN. In this case, the main event is routed in accordance with the workflow. A duplicate event is written to the database when one of the following conditions is satisfied:
	  • A status other than **Unclassified** is received from KSN.
	  • The disk buffer configured using the **Buffer size** setting is full.
	  • The **Request count** is exceeded.
	If this setting is disabled, KUMA continues to send requests using the main event. The event is written to the database when one of the following conditions is satisfied:
	• A status other than **Unclassified** is received from KSN.
	• The disk buffer configured using the **Buffer size** setting is full.
	• The **Request count** is exceeded.
	• The **Request count** is the maximum number of requests to KSN. If a status other than **Unclassified** is not received by executing the specified number of requests, the event is written to the database with the **Unclassified** status. The default value is `10`.
	• **Poll interval** is the interval between requests, in minutes. The default value is `1 minute`. The minimum value is `1 minute`.
	• **Buffer size** is the size of the disk buffer for events awaiting a repeat request, in megabytes. The default value is `10240 MB`. The minimum value is `10 MB`.

Proxy server	Proxy server settings, if one is needed to connect to the KSN server. You can select one of the available proxy servers or create a new proxy server. By default, a proxy server is not used.
Mapping	The table of parameters that must be sent in a KSN request to get a status, and a list of the corresponding KUMA event fields. • **DLL file hash (md5)**—a recommended mapping field: `OldFileHash`. • **DLL file path**—a full path including a file name. Recommended field for mapping: `OldFilePath`. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **Process hash (md5)**—a recommended mapping field: `FileHash`. • **process path**. Full path including the file name. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **DLL file name**—a recommended mapping field: `OldFileName`. • **Process name**—a recommended mapping field: `FileName`. • **Process signature** is a field that specifies the KUMA field that transfers the `Organization` from the signature `Subject`. If these values are not available, leave the signature empty. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** column, select **process signature** from the drop-down list (optional). Recommended field for mapping: FileID. • **dll size**. Optional; recommended field for mapping: OldFileSize. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** field, select **dll size** from the drop-down list. For each parameter, specify a corresponding KUMA event field in the table.

d. In the **Target field** drop-down list, select the KUMA event field to which you want to write the data. You cannot select a value if in the **Source kind** drop-down list, you selected **table**.

e. If you want to enable details in the normalizer log, enable the **Debug** toggle switch. The toggle switch is turned off by default.

6. Click **OK**.

The normalizer is created and displayed as a dark circle on the **Event parsing** tab of the Installation Wizard. You can click the dark circle to view the settings of the normalizer. If you want to edit additional parsing settings, hover over the dark circle and click the plus symbol that appears. This opens the **Additional event parsing** with settings of the additional parsing. For more details on configuring the additional parsing of events, see the **Creating the structure of event normalization rules** section below.

When displaying a normalization scheme, the structure of nested normalizers is not displayed. To view this structure, you need to go to the normalizer card by clicking its name link. If you are using a nested normalizer with extra normalization, keep in mind that the structure of the output data may change. In that case, it is important to understand which field is passed to the other extra normalizer.

4 Adding a filter (optional step)

You can create a filter that defines the conditions for event selection. You can add multiple filters to the collector. You can swap the filters by dragging them by the ⠿ icon as well as delete them. Filters are combined by the AND operator.

When configuring filters, we recommend to adhere to the chosen normalization scheme. In filters, use only KUMA service fields and the fields that you specified in the normalizer in the **Mapping** and **Enrichment** sections. For example, if the `DeviceAddress` field is not used in normalization, avoid using the `DeviceAddress` field in a filter as such filtering will not work.

To create a filter:

1. In the **Event filtration** section, click the **Add filter** button, and select **Create** from the **Filter** drop-down menu.

2. If you want to keep the filter as a separate resource, select the **Save filter** check box. This can be useful if you decide to reuse the same filter across different services. This check box is cleared by default.

3. If you selected the **Save filter** check box, enter a name for the created filter in the **Name** field. The name must contain 1 to 128 Unicode characters.

4. In the **Conditions** settings block, specify the conditions that filtered events must meet:

   You can click the **Add condition** button to add filtering conditions. You can select two values (two operands, left and right) and assign the operation you want to perform with the selected values. The result of the operation is either True or False.

   a. In the **op** drop-down list, select the function to be performed by the filter.

      In this drop-down list, you can select the **do not match case** check box if the operator should ignore the case of values. This check box is ignored if the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup** operators are selected. This check box is cleared by default.

      Filter operators

      - **=** means the left operand equals the right operand.
      - **<** means the left operand is less than the right operand.
      - **<=** means the left operand is less than or equal to the right operand.
      - **>** means the left operand is greater than the right operand.
      - **>=** means the left operand is greater than or equal to the right operand.
      - **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
      - **contains** means the left operand contains values of the right operand.
      - **startsWith** means the left operand starts with one of the values of the right operand.

- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
- **inContextTable** checks for the presence of the entry in the specified context table.
- **intersect**—presence in the left operand of the list items specified in the right operand.

b. In the **Left operand** and **Right operand** drop-down lists, select where the data to be filtered will come from. As a result of the selection, advanced settings are displayed, which you can use to precisely define the value to be passed to the filter. For example, when choosing **active list** you will need to specify the name of the active list, the entry key, and the entry key field.

c. You can use the **If** drop-down list to choose whether you need to create a negative filter condition.

   Conditions can be deleted using the × button.

d. The **Add group** button is used to add groups of conditions. The **AND** can be switched between **And**, **OR**, **NOT**.

   A condition group can be deleted using the × button.

e. By clicking **Add filter**, you can add existing filters selected in the **Select filter** drop-down list to the conditions. You can click ↗ to navigate to a nested filter.

The filter has been added. You can delete it using the × button.

5 Adding an aggregation rule (optional step)

1. In the **Event aggregation** section, click **Add aggregation rule**.

2. In the **Aggregation rule** drop-down menu, select the required rule or create a new one by clicking **New**.

3. Enter the name of the newly created aggregation rule in the **Name** field. The name must contain 1 to 128 Unicode characters.

4. In the **Threshold** field, specify how many events must be accumulated before the aggregation rule triggers and the events are aggregated. The default value is `100`.

5. In the **Triggered rule lifetime** field, specify how long (in seconds) the collector must accumulate events to be aggregated. When this time expires, the aggregation rule is triggered and a new aggregation event is created. The default value is `60`.

6. In the **Identical fields** section, use the **Add field** button to select the fields that will be used to identify the same type events. You can select the following service fields: SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID. Asset IDs are added after event normalization, which means you can use them to aggregate events. The rest of the service fields are not used in aggregation. Selected events can be deleted using the buttons with a cross icon.

7. In the **Unique fields** section, you can click **Add field** to select the fields that will cause the collector to disqualify events from aggregation even if the events contain fields listed in the **Identical fields** section. Selected events can be deleted using the buttons with a cross icon.

8. In the **Sum fields** section, you can use the **Add field** button to select the fields whose values will be summed during the aggregation process. Selected events can be deleted using the buttons with a cross icon.

9. In the **Filter** settings block, you can specify the conditions to define events that will be processed by this resource. You can select an existing filter from the drop-down list or **create** a new filter.

   Creating a filter in resources

   All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

   To create a filter:

   1. In the **Filter** drop-down list, select **Create new**.

   2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

   3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

   4. Select the filter creation mode: **Constructor** or **Code**.

      When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

5. If you selected the **Constructor** option, do the following:

   a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.
      - **OR**: selects events that match one of the specified conditions.
      - **NOT**: selects events that match none of the specified conditions.

   b. Click the **Add condition** button.

   c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

   d. From the drop-down lists, select operands and filter operators.

      Operands of filters

      - **Event fields** specify the field of the event that you need to use as a filter operand.
      - **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

        If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
      - **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
        - **dictionary** (required) is the dictionary that you want to use.
        - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
      - In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
        - **context table name** (required) is the context table that you want to use.
        - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
        - **field** is the name of the context table field from which you want to get the value of the operand.
        - **index** is the index of the list field of the table from which you want to get the value of the operand.
      - **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
        - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
        - **key fields** (required) are event fields that are used to generate the key of the dictionary value.

- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.

- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
- **inContextTable** checks for the presence of the entry in the specified context table.
- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ×.

8. Click **Save**.

Aggregation rule is added. You can delete it using the × button.

6 Event enrichment (optional step)

You can specify which data, and from which sources, are added to events that are processed by the collector. Events can be enriched with data obtained using enrichment rules or LDAP.

Incoming events are first enriched with data from the sources that you select at this step of the wizard, and then the events are automatically enriched with asset information. For example, if you have dns enrichment configured, which leads to the IP address in the event being enriched with the corresponding DNS name of an asset, the event is enriched with this asset.

The collector receives information about assets from the KUMA Core and enriches events with this information as follows:

- If the name field of the event (for example, `SourceHostName`) contains an FQDN that matches the FQDN of an asset, the collector adds a `SourceAssetID` field with the ID of thif asset. This does not take into account the value of the `SourceAddress` field.
- If an IP address field of an event (for example, `DestinationAddress`) includes the IP address of an asset, and the name field is empty, the collector adds a `DestinationAssetID` field with the ID of the asset that has the matching IP address.
- If a name field of an event does not match any FQDN from the asset database, the collector does not check the IP address field or add an asset ID. This applies to cases in which the `HostName` field contains an FQDN that does not match any asset, as well as cases in which an incomplete name is specified in the `HostName` field (for example, only the host name without a domain).

There can be more than one enrichment rule. You can add them by clicking the **Add enrichment** button and can remove them by clicking the ✕ button. You can use existing enrichment rules or create new rules.

To create an enrichment rule:

1. In the web interface, open the **Event enrichment** section.
2. Depending on what you want to use to enrich events, do the following:
   - To enrich events with data obtained using enrichment rules:
     a. Click **Add enrichment**.
     This opens the enrichment rules settings block.
     b. In the **Name** field, enter a unique name for the rule. The name must contain 1 to 128 Unicode characters.
     c. In the **Enrichment rule** drop-down list, select **Create new**.
     d. In the **Source kind** drop-down list, select the source of data for enrichment and define its corresponding settings:
     template
     This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

table

This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "table"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.
Mapping	Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`).

The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field.

If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

enrichment by assets

You can use this type of enrichment when you need to add enrichment of events with assets to specific collectors.

To enrich events with assets in the **Mapping** block, fill in the mapping table of the KUMA event fields and the fields used to record values from the hash table.

To fill in the field mapping table:

1. In the **Matching** block, click **Add**.

2. In the **KUMA field** drop-down list, select one or more event fields that you want to map to values from the hash table and write to the corresponding field in the asset information table.

3. In the **Field to write data to** drop-down list, select the field into which the asset ID value will be written when the event field (**KUMA field**) matches the value from the hash table.

   Possible parameter values in the field mapping table

KUMA field	KUMA event field to write to

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

   When you specify multiple fields, the **AND** operator is applied to field values. If you add multiple strings in the **KUMA field** column, the **OR** operator is applied to field values. The matching begins from the first field in the list. If the value of the field matches the value of the attribute, matching stops.

   For example, suppose that the following data is received in an event:

   `SourceAddress=192.168.x.xx`
   `SourceHostName=kuma.example.com`

   There are two assets in KUMA: `company.example.com` (IP address: `192.168.x.xx`; FQDN: `company.example.com`) and `kuma.example.com` (IP address: `192.168.y.yyy`; FQDN: `kuma.example.com`). Matching is performed as follows:

   - If you specify `sourceAddress` → `sourceAssetID`, and then `sourceHostname` → `sourceAssetID` separately, then the asset will correspond to the first condition (`company.example.com`).

   - If it is more important to get the `sourceHostname` parameter value (`kuma.example.com`), then `sourceHostname` → `sourceAssetID` must be specified first followed by `sourceAddress` → `sourceAssetID`.

   - If you specify `sourceAddress` + `sourceHostname` → `sourceAssetID`, there will be no enrichment.

   > At least one matching condition must be specified in the field mapping table.

4. To apply the default values for the **KUMA field** and **Field for data recording** parameters, click the button. **Apply the default mapping** located above the table.

   Default parameter values

KUMA field	KUMA event field to write to
`DestinationAddress`	`DestinationAssetID`
`DestinationHostName`	`DestinationAssetID`
`DeviceAddress`	`DeviceAssetID`
`DeviceHostName`	`DeviceAssetID`
`SourceAddress`	`SourceAssetID`
`SourceHostName`	`SourceAssetID`

constant

This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "constant"

Setting	Description
Constant	The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed.
Target field	The event field to insert the data into.

If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field.

If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array.

dictionary

This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dictionary"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.

If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`.

If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`.

event

This type of enrichment is used when you need to write a value from another event field to the current event field. The settings of the enrichment type are described in the table below.

Parameters of enrichment type "event"

Setting	Description
Target field	The event field where the data needs to be inserted.
Source field	The event field whose value is written to the target field.
Conversion	The block of settings where you can create rules for modifying the original data before it is written to event fields. The conversion type can be selected from the drop-down list. You can use the **Add conversion** and **Delete** buttons to add or delete a conversion, respectively. The order of conversions is important.

Whether or not a conversion can be used depends on the type of an extended event schema field being used:

- For an additional field of the `String` type, all types of conversion are available.
- For the `Number` and `Float` type fields, the following types of conversion are available: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String**, and **decodeBase64URLString**.
- For the `Array of strings`, `Array of numbers`, and `Array of floats` type fields, the following types of conversion are available: **append**, and **prepend**.

View available transformations

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.
- **lower**—is used to make all characters of the value lowercase
- **upper**—is used to make all characters of the value uppercase
- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.
- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.
- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:
  - **Replace chars** specifies the sequence of characters to be replaced.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:

  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.

  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

dns

This type of enrichment is used to send requests to a private network DNS server to convert IP addresses into domain names or vice versa. IP addresses are converted to DNS names only for private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dns"

Setting	Description
URL	URL of the DNS server to which you want to send requests. You can use the **Add URL** button to specify multiple URLs. If the **URL** setting is not specified, KUMA takes the list of DNS servers from the localhost's `/etc/resolv.conf` file. In this case, you need to enable the **Recursive queries** option. Otherwise, the enrichment will not occur.
Requests per second	Maximum number of queries sent to the DNS server per second. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Workers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used. The default value is `1`.
Maximum number of events in enrichment queue	The maximum number of events to hold in the resubmission queue. The default value is `1,000,000`.
Timeout	The time to wait for a response from the DNS server (in seconds). The default value is `5`.
DNS mode override	Resolution method used: • **Forward DNS only** resolves a domain name to an IP address. • **Reverse DNS only** resolves an IP address to a domain name. • **Forward and reverse DNS** resolves a domain name to an IP address or an IP address to a domain name.
Cache TTL	The lifetime (in seconds) of values stored in the cache. The default value is `60` seconds.
Cache disabled	You can enable or disable caching using this setting. Caching is enabled by default.
Cache refresh disabled	If cache update is enabled, then upon expiry of the cache's TTL the collector sends repeated requests to the DNS server to update the data stored in the cache. This setting is available only when cache is enabled. By default, cache update is enabled.
Recursive queries	Allows a collector to send recursive queries to authoritative DNS servers for the purposes of enrichment. The default value is **Disabled**.

cybertrace

For systems with high load on a collector or correlator, we recommend using the **cybertrace-http** enrichment type. This type of enrichment returns a structured JSON response and correctly distinguishes between strings and arrays of custom attributes, preventing parsing errors.
When **cybertrace** enrichment is used, the collector receives an unstructured response. If the value of a custom attribute in Kaspersky CyberTrace contains square brackets, for example, **[str1**, **str2]**, Kaspersky SIEM treats it as an array, not a string.

This type of enrichment is used to add information from Kaspersky CyberTrace data feeds to event fields. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace"

Setting	Description
URL	URL of the Kaspersky CyberTrace server which you want to send requests to. The default Kaspersky CyberTrace port is 9999. Required setting.
Number of connections	Maximum number of connections to the Kaspersky CyberTrace server that can be established simultaneously by Kaspersky SIEM. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Requests per second	Maximum number of requests sent to the server per second. The default value is `1000`.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`.
Mapping	Table for mapping event fields to the types of indicators in Kaspersky CyberTrace. The **KUMA field** column shows the names of event fields, and the **CyberTrace indicator** column shows the types of Kaspersky CyberTrace indicators. Available types of Kaspersky CyberTrace indicators: • **ip** • **url** • **hash**

In the mapping table, you must provide at least one string. You can add new table rows or delete table rows. To add a new table row, click **Add row**. To delete a row in the table, click the ✕ cross.

cybertrace-http

This streaming event enrichment type in Kaspersky CyberTrace allows you to send a large number of events to the CyberTrace API-interface with a single request. We recommend using the **cybertrace-http** enrichment type for systems with a large stream of events. The **cybertrace-http** enrichment type performs better than the **cybertrace** enrichment type.

Limitations:

- The **cybertrace-http** enrichment type cannot be used for retrospective scanning in KUMA.
- When the **cybertrace-http** enrichment type is used, cyberthreat detections are not saved in Kaspersky CyberTrace history in the **Detections** window.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace-http"

Setting	Description
Tenant	Tenant, within which you plan to work with Kaspersky CyberTrace. Required setting.
URL	URL of the Kaspersky CyberTrace server to which you want to send requests, and the port used by the CyberTrace API. The default port is 443. Required setting.
Secret	The drop-down list where you can select the secret that stores the connection credentials. Required setting.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Key fields	The list of event fields used for enriching events with data from Kaspersky CyberTrace. Required setting.

Setting	Description
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`. After reaching 1 million events received from the Kaspersky CyberTrace server, events stop being enriched until the number of received events is reduced to less than 500,000.
CyberTrace main version	Kaspersky CyberTrace version. Available values: • **<5**—requests are executed in the General tenant in Kaspersky CyberTrace, and use the new API version provided by Kaspersky CyberTrace 5.0 and later. • **≥ 5.0**—requests use the API version that corresponds to Kaspersky CyberTrace 4.x. The default value is **<5**.
Debug	The parameter that enables resource logging. The toggle switch is turned off by default.
Tags	Tags for resource search.

timezone

This type of enrichment is used in collectors and correlators to assign a specific time zone to an event. Time zone information may be useful when searching for events that occurred at unusual times, such as nighttime.

When this type of enrichment is selected, the required time zone must be selected from the **Time zone** drop-down list.

> Make sure that the selected time zone is set on the server hosting the enrichment-utilizing service. For example, you can do this by using the `timedatectl list-timezones` command, which shows all time zones that are set on the server. For more details on setting time zones, please refer to your operating system documentation.

When an event is enriched, the time offset of the selected time zone relative to Coordinated Universal Time (UTC) is written to the DeviceTimeZone event field in the `+-hh:mm` format. For example, if you select the **Asia/Yekaterinburg** time zone, the value `+05:00` will be written to the `DeviceTimeZone` field. If an enriched event already has a value in the `DeviceTimeZone` field, it will be overwritten.

By default, if the timezone is not specified in the event being processed and enrichment rules by timezone are not configured, the event is assigned the timezone of the server hosting the service (collector or correlator) that processes the event. If server time is changed, the service must be restarted.

Permissible time formats when enriching the DeviceTimeZone field

When processing incoming raw events in the collector, the following time formats can be automatically converted to the `+-hh:mm` format (see the table below):

Time format in a processed event	Example
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

If the date format in the `DeviceTimeZone` field differs from those listed in the table, the collector server time zone is written to the field when an event is enriched with time zone information. You can create normalization rules for non-standard time formats.

geographic data

This type of enrichment is used to add IP address geographic data to event fields.

When this type is selected under **Mapping geographic data to event fields** parameter block, you need to specify from which event field the IP address will be read, select the attributes of geographic data, and define the event fields to which geographic data will be written:

1. In the **Event field with IP address** drop-down list, select the event field from which the IP address is read. Geographic data uploaded to KUMA is matched against this IP address.

   When the `SourceAddress`, `DestinationAddress`, and `DeviceAddress` event fields are selected, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields.

2. For each event field you need to read the IP address from, select the type of geographic data and the event field to which the geographic data should be written.

   - In the **Geodata attribute** field, select which geographic data corresponding to the read IP address should be written to the event. Available geographic data attributes: **Country**, **Region**, **City**, **Longitude**, **Latitude**.

   - In the **Event field to write to**, select the event field which the selected geographic data attribute must be written to.

   You can use the **Add geodata attribute** button to add field pairs for **Geodata attribute** – **Event field to write to**. You can also configure different types of geographic data for one IP address to be written to different event fields.

3. To add each subsequent mapping, click the **Add mapping** button and repeat the previous two steps of these instructions.

   You can write identical geographic data attributes to different event fields. If you configure multiple geographic data attributes to be written to the same event field, the event will be enriched with the last mapping in the sequence.

check DLL Hijacking

DLL Hijacking is an attack technique that involves delivering vulnerable legitimate software along with a malicious dynamic link library (DLL) to a target system. To detect such attacks, Kaspersky SIEM uses the AI module. The AI module analyzes the launch and runtime parameters of applications and identifies suspicious launches of legitimate software with malicious libraries.

To get a status, Kaspersky SIEM sends a request with information from event fields to <KSN>. In response to the request, KSN sends the analysis result.

You can configure DLL Hijacking attack detection in the collector or correlator.

To use enrichment such as **check DLL Hijacking**, your license must include the AI module. The General administrator needs also to accept the additional KSN Statement in the **Kaspersky Security Network** section (**Settings** → **Integrations** → **AI services** → **DLL Hijacking detection**).

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "DLL Hijacking"

Setting	Description
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.

Maximum cache size	Maximum cache size for KSN responses, in megabytes. The default value is `128 MB`. Each KSN response has its own lifetime, during which it is retained in the cache. If Kaspersky SIEM sends a second request for a DLL file for which KSN has already issued a response, and the lifetime of that response has not yet expired, the request is not actually sent to KSN, but the response is taken from the cache.
Maximum number of events in enrichment queue	If the specified value is exceeded, new events are not processed. The default value is `1,000,000`. `0` means that event processing stops if the queue contains any number of events.

Perform a repeat request	KSN response may return the **Unclassified** status. This status means that KSN has accepted the request and is currently processing it, but there is no status yet. Processing may take a long time, so the request must be re-sent.
	If this setting is enabled, specify additional settings:
	• If the **Create duplicates** setting is enabled, KUMA creates a duplicate event and uses it for repeated requests to KSN. In this case, the main event is routed in accordance with the workflow. A duplicate event is written to the database when one of the following conditions is satisfied:
	  • A status other than **Unclassified** is received from KSN.
	  • The disk buffer configured using the **Buffer size** setting is full.
	  • The **Request count** is exceeded.
	If this setting is disabled, KUMA continues to send requests using the main event. The event is written to the database when one of the following conditions is satisfied:
	• A status other than **Unclassified** is received from KSN.
	• The disk buffer configured using the **Buffer size** setting is full.
	• The **Request count** is exceeded.
	• The **Request count** is the maximum number of requests to KSN. If a status other than **Unclassified** is not received by executing the specified number of requests, the event is written to the database with the **Unclassified** status. The default value is `10`.
	• **Poll interval** is the interval between requests, in minutes. The default value is `1 minute`. The minimum value is `1 minute`.
	• **Buffer size** is the size of the disk buffer for events awaiting a repeat request, in megabytes. The default value is `10240 MB`. The minimum value is `10 MB`.

Proxy server	Proxy server settings, if one is needed to connect to the KSN server. You can select one of the available proxy servers or create a new proxy server. By default, a proxy server is not used.
Mapping	The table of parameters that must be sent in a KSN request to get a status, and a list of the corresponding KUMA event fields. • **DLL file hash (md5)**—a recommended mapping field: `OldFileHash`. • **DLL file path**—a full path including a file name. Recommended field for mapping: `OldFilePath`. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **Process hash (md5)**—a recommended mapping field: `FileHash`. • **process path**. Full path including the file name. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **DLL file name**—a recommended mapping field: `OldFileName`. • **Process name**—a recommended mapping field: `FileName`. • **Process signature** is a field that specifies the KUMA field that transfers the `Organization` from the signature `Subject`. If these values are not available, leave the signature empty. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** column, select **process signature** from the drop-down list (optional). Recommended field for mapping: FileID. • **dll size**. Optional; recommended field for mapping: OldFileSize. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** field, select **dll size** from the drop-down list. For each parameter, specify a corresponding KUMA event field in the table.

e. If you want to enable logging of service operations, turn on the **Debug** toggle switch.

f. If necessary, in the **Tags** drop-down list, select thetags for the enrichment rule.

g. If required, add a description for the enrichment rule in the **Description** field. The rule description can contain up to 4000 Unicode characters.

h. If you want to specify conditions that define which events are processed by the enrichment rule, in the **Filter settings** section, select or create a filter from the **Filter** drop-down list.

How to create a filter

All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

To create a filter:

1. In the **Filter** drop-down list, select **Create new**.

2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

4. Select the filter creation mode: **Constructor** or **Code**.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

5. If you selected the **Constructor** option, do the following:

   a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

   b. Click the **Add condition** button.

   c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

   d. From the drop-down lists, select operands and filter operators.

      Operands of filters

      - **Event fields** specify the field of the event that you need to use as a filter operand.

      - **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

        If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.

- **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the dictionary that you want to use.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
  - **context table name** (required) is the context table that you want to use.
  - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
  - **field** is the name of the context table field from which you want to get the value of the operand.
  - **index** is the index of the list field of the table from which you want to get the value of the operand.
- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.

- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
- **inContextTable** checks for the presence of the entry in the specified context table.
- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⣿. To remove a condition, click the delete icon ×.

8. Click **Save**.

- If you want to enrich events with data obtained via LDAP, do the following:

a. Click **Add enrichment with LDAP data**.

This opens the group of settings for LDAP enrichment.

b. In the **LDAP accounts mapping** field, add one or more LDAP connections created in the LDAP server integration settings.

c. In the **LDAP mapping** table, define the rules for mapping KUMA fields to LDAP attributes:

- In the **KUMA field** column, indicate the KUMA event field whose data should be compared to an LDAP attribute.

- In the **LDAP attribute to receive** column, specify the attribute that must be compared to the KUMA event field. The drop-down list contains some of the standard attributes that can be used for enrichment. You can add custom attributes to the list.

Configuring enrichment using custom attributes

Before configuring event enrichment using custom attributes, make sure that custom attributes are configured in AD.

To enrich events with accounts using custom attributes:

1. Add **Custom AD Account Attributes** in the LDAP connection settings.

Default imported attributes from AD cannot be added as custom attributes. For example, if you add the standard `accountExpires` attribute as a custom attribute, KUMA returns an error when saving the connection settings.

List of attributes imported from AD

The following account attributes can be requested from Active Directory:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `company`

- `department`
- `displayName`
- `distinguishedName`
- `division`
- `employeeID`
- `ipaUniqueID`
- `l`
- `mail`
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (this attribute can be used for search during correlation)
- `mobile`
- `objectGUID` (this attribute always requested from Active Directory even if a user doesn't specify it)
- `objectSid`
- `physicalDeliveryOfficeName`
- `sAMAccountName`
- `sAMAccountType`
- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `userPrincipalName`
- `whenChanged`
- `whenCreated`

After you add custom attributes in the LDAP connection settings, the **LDAP attributes** drop-down list in the collector will be automatically appended with new attributes. Custom attributes are identified by a question mark next to the attribute name. If you added the same attribute for multiple domains, the attribute is listed only once in the drop-down list. You can view the domains by moving your cursor over the question mark. Domain names are displayed as links. If you click a link, the domain is automatically added to **LDAP accounts mapping** if it was not previously added.

If you deleted a custom attribute in the LDAP connection settings, delete the row containing the attribute from the collector's mapping table manually. Account attribute information in KUMA is updated each time you import accounts.

2. Import accounts.

3. In the collector, in the **LDAP mapping** table, define the rules for mapping KUMA fields to LDAP attributes.

4. Restart the collector.

   After the collector is restarted, KUMA begins enriching events with accounts.

- In the **Event field to write to** column, specify the KUMA event field where the ID of the user account imported from LDAP needs to be placed in case of successful mapping.

You can use the **Add** button to add a row to the table, and remove one using the **Delete** button. You can use the **Apply default mapping** button to fill the mapping table with standard values.

> If you add an enrichment using LDAP to an existing collector or change the enrichment settings, you must stop and restart the service.

7 Add destination (optional step)

You can select or create destinations with settings indicating the forwarding destination for events processed by the collector. Typically, events from the collector are routed to the correlator to analyze and search for threats; and to the storage, both for storage and so that processed events can be viewed later. If necessary, you can send events to an event router. In this case, select the `internal` connector at the **Transport** step. There can be more than one destination point.

To add a destination:

1. In the **Routing** section, click **Add**.

2. In the **Create destination** window, in the **Destination** field, select the destination type that you want to add, or create a new one by clicking **New** and configuring the following settings:

   a. On the **Basic settings** tab, in the **Name** field, enter a unique name for the destination. The name must contain 1 to 128 Unicode characters.

   b. You can use the **State** toggle switch to enable or disable the service as needed.

c. In the **Type** drop-down list, select the type of the destination. The following values are available:

- internal
- nats-jetstream
- tcp
- udp
- http
- diode
- kafka
- file
- storage
- correlator
- eventRouter

d. On the **Advanced settings** tab, specify the values of parameters. The set of parameters that can be configured depends on the type of the destination selected on the **Basic settings** tab. For detailed information about parameters and their values, click the link for each type of destination in paragraph "c." of these instructions.

The created destination is displayed on the Installation Wizard tab. A destination resource can be removed from the resource set by selecting it and clicking **Delete** in the opened window.

8 Collector setup validation

At this stage, KUMA creates a service resource set with the services being created automatically based on this set:

- The resource set for the collector is displayed under **Resources** → **Collectors**. It can be used to create new collector services. When this set of resources changes, all services that operate based on this set of resources will start using the new parameters after the services restart. To do so, you can use the **Save and restart services** and **Save and update service configurations** buttons.

  A resource set can be modified, copied, moved from one folder to another, deleted, imported, and exported, like other resources.

- Services are displayed in **Resources** → **Active services**. The services created using the Installation Wizard perform functions inside the KUMA solution. To communicate with external parts of the network infrastructure, you need to install similar external services on the servers and assets intended for them. For example, an external collector service should be installed on a server intended as an events recipient, external storage services should be installed on servers that have a deployed ClickHouse service, and external agent services should be installed on the Windows assets that must both receive and forward Windows events.

To check the collector settings:

1. In the **Setup validation** section, click **Create and save service**.

   A table of services that are created based on the set of resources selected in the installation wizard appears. The lower part of the window shows examples of commands to be used to install external equivalents of these services on their intended servers and assets.

   Example

   ```
   /opt/kaspersky/kuma/kuma collector --core https://kuma-example:<port used for communication with the KUMA Core>
   --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <port used for
   communication with the service> --install
   ```

   where:

   `<fingerprint ID of the KUMA Core CA certificate>` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

   The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
   You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

   To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

   > The `kuma` file can be found inside the installer in the `/kuma-ansible-installer/roles/kuma/files/` directory.

   The port for communication with the KUMA Core, the service ID, the fingerprint ID of the CA certificate, and the port for communication with the service are added to the command automatically. You should also ensure the network connectivity of the KUMA system and open the ports used by its components if necessary.

2. Close the collector creation window by clicking **Save collector**.

   The collector service will be created in KUMA. Now the service must be installed on the server intended for receiving events.

> If a WEC, WMI, or ETW connector was selected for the collector, you must also install the automatically created KUMA agents.

Once the collector is created and configured, install the KUMA collector on the server.

Installing the collector on the server

After creating a collector, install it on a server in the network infrastructure used to receive events.

To install a collector:

1. Log in to the server where you want to install the service.

2. Get the service ID. To do this, in the web interface, go to **Resources** → **Active services**, and in the context menu of the KUMA Core, click **Copy ID**.

3. Execute the following command:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --api.port <API_port>
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.

- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).

- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

- <service_ID> is the router ID copied from the KUMA web interface.

- <API_port> is the port used for communication with the component being installed.

Example

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
--api.port YYYY
```

If errors are detected as a result of the command execution, make sure that the settings are correct. For example, the availability of the required access level, network availability between the collector service and the Core, and the uniqueness of the selected API port. After fixing errors, continue installing the collector.

If no errors were found, and the collector status in the KUMA web interface is changed to *green*, stop the command execution and proceed to the next step.

> The command can be copied at the last step of the installer wizard. The address and port of the KUMA Core server, the identifier of the collector to be installed, the fingerprint ID of the CA certificate, and the port that the collector uses for communication are automatically specified in the command.

When deploying several KUMA services on the same host, during the installation process you must specify unique ports for each component using the `--api.port <API_port>` option. The following setting values are used by default: `--api.port 7221`.

Before installation, check the network connectivity of KUMA components.

4. Run the command again by adding the `--install` key:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --api.port <API_port> --install
```

Example

```
sudo /opt/kaspersky/kuma/kuma collector --core https://example.com:7210 --pair.fingerprint XXXX --id XXXX --
api.port YYYY --install
```

5. Add KUMA collector port to firewall exclusions.

For the solution to work correctly, ensure that the KUMA components are able to interact with other components and applications over the network via the protocols and ports specified during the installation of the KUMA components.

The collector is installed. You can use it to receive data from an event source and send it for processing.

6. In the **Resources** → **Active services** section, make sure that the collector you installed has a green status.

   If the status of the collector is not green, view the log of this service on the computer where it is installed under `/opt/kaspersky/kuma/collector/<collector ID>/log/collector directory`. Errors are logged regardless of whether debug mode is enabled or disabled.

If the collector is installed correctly and you are sure that data is coming from the event source, the table should display events when you search for events associated with the collector.

To check for normalization errors using the Events section of the KUMA web interface:

1. Make sure that the Collector service is running.

2. Make sure that the event source is providing events to the KUMA.

3. Make sure that in the in the **Resources** section of the KUMA web interface, in the **Keep raw event** drop-down list for the **Normalizer** resource, you have selected **Only errors**.

4. In the **Events** section of KUMA, search for events with the following parameters:

```
ServiceID = <ID of the collector to be checked>
Raw != ""
```

If any events are found with this search, it means that there are normalization errors and they should be investigated.

To check for normalization errors using the KUMA Collectors Dashboard:

1. Make sure that the Collector service is running.
2. Make sure that the event source is providing events to the KUMA.
3. In the **Metrics** section, follow the **KUMA Collectors** link.
4. Check if the **Errors** section of the **Normalization** widget displays any errors.

   If there are any errors, it means that there are normalization errors and they should be investigated.

For collectors that use WEC, WMI, or ETW connectors as the transport, make sure that a unique port is used for connecting to the agent. This port is specified in the **Transport** section during creation of the collector.

Ensuring uninterrupted collector operation

An uninterrupted event stream from the event source to KUMA is important for protecting the network infrastructure.

To configure uninterrupted event stream, follow the steps below:

1 Collector installation

On the KUMA side, install two or more identical collectors.

2 Configuring the event streams among the collectors

On the event source side, configure the event streams management between collectors using third-party server load management tools.

1. If you want to manage the event stream using rsyslog, do the following:

   a. Install rsyslog on the event source server (refer to the rsyslog documentation).

   b. Add rules for forwarding the event stream between collectors to the configuration file `/etc/rsyslog.conf`:

   ```
   *.* @@<main collector server FQDN>:<port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended on
   & @@<backup collector server FQDN>:<port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   Example configuration file

   Example configuration file specifying one primary and two backup collectors. The collectors are configured to receive events on TCP port 5140.

```
*.* @@kuma-collector-01.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended on
& @@kuma-collector-02.example.com:5140
& @@kuma-collector-03.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended off
```

c. Restart the rsyslog service using the following command:

```
systemctl restart rsyslog
```

2. If you want to manage the event stream using nginx, do the following:

a. Install nginx on the server for event stream management using one of the commands:

- Installation command in Oracle Linux 8.6:

```
$sudo dnf install nginx
```

- Installation command in Ubuntu 20.4:

```
$sudo apt-get install nginx
```

When installing from sources, you must compile with the parameter `-with-stream` option: `$ sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

b. On the nginx server, add the stream module to the `nginx.conf` `configuration` file that contains the rules for forwarding the stream of events between collectors.

Example stream module

Example module in which event stream is distributed between the collectors kuma-collector-01.example.com and kuma-collector-02.example.com, which receive events via TCP on port 5140 and via UDP on port 5141. Balancing uses the nginx.example.com ngnix server.

```
stream {
 upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
 server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
 worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile is the limit on the number of open files (RLIMIT_NOFILE) for workers. This is used to raise the limit without restarting the main process.
# worker_connections is the maximum number of connections that a worker can open simultaneously.
```

With a large number of active services and users, you may need to increase the limit of open files in the `nginx.conf` settings.

Example

```
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
```

where:

- `worker_rlimit_nofile` is the limit on the number of open files (RLIMIT_NOFILE) for workers. This is used to raise the limit without restarting the main process;
- `worker_connections` is the maximum number of connections that a worker can open simultaneously.

c. Restart nginx by running the following command:

```
systemctl restart nginx
```

d. On the event source server, forward events to the nginx server.

Nginx Plus may be required to fine-tune balancing, but certain balancing methods, such as Round Robin and Least Connections, are available in the base version of ngnix.

For more details on configuring nginx, please refer to the nginx documentation.

With this configuration of the collectors in place, no incoming events will be lost if the collector server is unavailable for any reason.

Please keep in mind that when the event stream switches between collectors, each collector will aggregate events separately.

3 Resolving errors (if necessary)

If the KUMA collector fails to start, and its log includes the `"panic: runtime error: slice bounds out of range [8:0]"` error, follow the steps below:

1. Stop the collector using the command:

```
sudo systemctl stop kuma-collector-<collector ID>
```

2. Delete the DNS enrichment cache files.

```
sudo rm -rf /opt/kaspersky/kuma/collector/<collector ID>/cache/enrichment/DNS-*
```

3. Delete the event cache files (disk buffer). Run the command only if you can afford to jettison the events in the disk buffers of the collector.

```
sudo rm -rf /opt/kaspersky/kuma/collector/<collector ID>/buffers/*
```

4. Start the collector service.

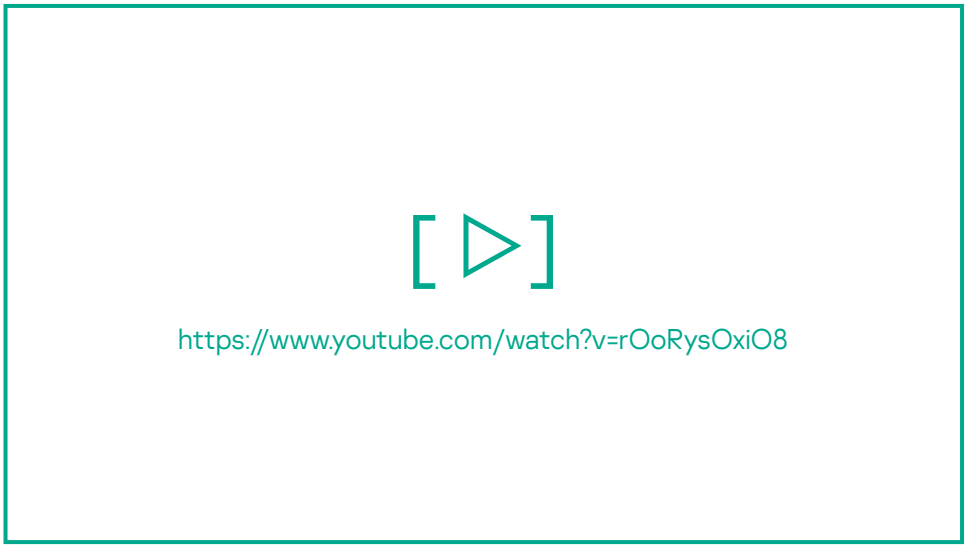
```
sudo systemctl start kuma-collector-<collector ID>
```

Event aggregation

Aggregation rules let you combine repetitive events of the same type and replace them with one common event. Aggregation rules support fields of the standard KUMA event schema as well as fields of the extended event schema. This way you can reduce the number of similar events sent to the storage and/or the correlator, reduce the workload on services, conserve data storage space and licensing quota (EPS). An aggregation event is created when a time or number of events threshold is reached, whichever occurs first.

For aggregation rules, you can configure a filter and apply it only to events that match the specified conditions.

To learn more about how aggregation rules work, watch this video:



The [OOTB] NetFlow 9 aggregation rule is included in the KUMA distribution kit. The rule is triggered after 100 events or 10 seconds.

Events are aggregated by the following fields:

- `DestinationAddress`
- `DestinationPort`
- `SourceAddress`
- `TransportProtocol`
- `DeviceVendor`
- `DeviceProduct`

The `DeviceCustomString1` and `BytesIn` fields are summed up.

To create an aggregation rule:

1. In the web interface, go to **Resources** → **Aggregation rules**, and click **New**.

2. Enter the name of the newly created aggregation rule in the **Name** field. The name must contain 1 to 128 Unicode characters.

3. In the **Tenant** drop-down list, select the tenant that owns the aggregation rule.

4. In the **Threshold** field, specify how many events must be accumulated before the aggregation rule triggers and the events are aggregated. The default value is `100`.

5. In the **Triggered rule lifetime** field, specify how long (in seconds) the collector must accumulate events to be aggregated. When this time expires, the aggregation rule is triggered and a new aggregation event is created. The default value is `60`.

6. In the **Description** field, enter a description of the aggregation rule. Maximum length of the description: 4000 Unicode characters.

7. In the **Identical fields** section, use the **Add field** button to select the fields that will be used to identify the same type events. You can select the following service fields: SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID. Asset IDs are added after event normalization, which means you can use them to aggregate events. The rest of the service fields are not used in aggregation. Selected events can be deleted using the buttons with a cross icon.

8. In the **Unique fields** section, you can click **Add field** to select the fields that will cause the collector to disqualify events from aggregation even if the events contain fields listed in the **Identical fields** section. Selected events can be deleted using the buttons with a cross icon.

If you specify more than one field under **Unique Fields**, the combinations of values of all of these fields must be unique.

Unique fields are not saved in the aggregated event.

9. In the **Sum fields** section, you can use the **Add field** button to select the fields whose values will be summed during the aggregation process. Selected events can be deleted using the buttons with a cross icon.

   The following special considerations are relevant to field behavior:

   - The values of fields of the `Number` and `Float` types are summed up.
   - The values of fields of the `String` type are concatenated with commas added as separators.
   - The values of fields with the types `Array of strings`, `Array of numbers` and `Array of floats` are appended to the end of the array.

10. In the **Filter parameters** settings block, specify the conditions to define events that will be processed by this rule. You can select an existing filter from the drop-down list or **create** a new filter.

    How to create a filter in resources

    All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

    To create a filter:

    1. In the **Filter** drop-down list, select **Create new**.
    2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.
    3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.
    4. Select the filter creation mode: **Constructor** or **Code**.

       When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.
    5. If you selected the **Constructor** option, do the following:

       a. In the drop-down list select a boolean operator:

       - **AND**: selects events that match all of the specified conditions.
       - **OR**: selects events that match one of the specified conditions.
       - **NOT**: selects events that match none of the specified conditions.

       b. Click the **Add condition** button.

       c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

       d. From the drop-down lists, select operands and filter operators.

Operands of filters

- **Event fields** specify the field of the event that you need to use as a filter operand.
- **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **Ctrl**/**Command**+**F1**.

  If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
- **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the dictionary that you want to use.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
  - **context table name** (required) is the context table that you want to use.
  - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
  - **field** is the name of the context table field from which you want to get the value of the operand.
  - **index** is the index of the list field of the table from which you want to get the value of the operand.
- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
- **inContextTable** checks for the presence of the entry in the specified context table.
- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **`Backspace`**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⣿. To remove a condition, click the delete icon ✕.

8. Click **Save**.

In aggregation rules, do not use filters with the **TI** operand or the **TIDetect**, **inActiveDirectoryGroup**, or **hasVulnerability** operators. The `Active Directory` fields for which you can use the **inActiveDirectoryGroup** operator will appear during the enrichment stage (after aggregation rules are executed).

11. Click the **Create** button.

After you create the aggregation rule, you can link it to the collector.

Normalization of events

Normalizers are used for converting raw events that come from various sources in different formats to the KUMA event data model. Normalized events become available for processing by other KUMA resources and services.

To learn more about how normalizers work, watch this video:

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

A normalizer consists of the *main* event parsing rule and optional *additional event parsing rules*. By creating a main parsing rule and a set of additional parsing rules, you can implement complex event processing logic. Data is passed along the tree of parsing rules depending on the conditions specified in the setting

Extra normalization conditions. The sequence in which parsing rules are created is significant: the event is processed sequentially and the processing sequence is indicated by arrows.
The following event normalization options are available:

- 1 collector—1 normalizer.

  We recommend using this method if you have many events of the same type or many IP addresses from which events of the same type may originate. You can configure one collector with only one normalizer, which is optimal in terms of performance.

- 1 collector—multiple normalizers linked to the IP address.

  This method is available for collectors with a connector of UDP, TCP, or HTTP type. If a UDP, TCP, or HTTP connector is specified in the collector at the 'Transport' step, then at the 'Event parsing' step, you can specify multiple IP addresses on the 'Parsing settings' tab and choose the normalizer that you want to use for events coming from the specified addresses. The following types of normalizers are available: json, cef, regexp, syslog, csv, kv, xml. For normalizers of the Syslog and regexp types, you can specify extra normalization conditions depending on the value of the DeviceProcessName field.

To create a normalizer:

1. In the web interface, go to **Resources** → **Normalizers** and click the **Create** button.

2. In the **Name** field, enter a unique name for the normalizer. Maximum length of the name: 128 Unicode characters.

3. In the **Tenant** drop-down list, select the tenant to which the normalizer belongs.

4. In the **Parsing method** drop-down list, select the type of events to receive. Depending on the selected value, you can use the predefined event field matching rules or define rules manually. When you select some parsing methods, additional settings may become available that you must specify.

   Available parsing methods:

   json

   This parsing method is used to process JSON data where each object, including its nested objects, occupies a single line in a file.

   When processing files with hierarchically structured data, you can reference the fields of nested objects using the dot notation. For example, the `username` parameter from the string `"user": {"username": "system: node: example-01"}` can be accessed by using the `user.username` query.

   Files are processed line by line. Multi-line objects with nested structures may be normalized incorrectly.

   In complex normalization schemes where additional normalizers are used, all nested objects are processed at the first normalization level, except for cases when the extra normalization conditions are not specified and, therefore, the event being processed is passed to the extra normalizer in its entirety.

   You can use `\n` and `\r\n` as newline characters. Strings must be UTF-8 encoded.

   If you want to send the raw event for advanced normalization, at each nesting level in the **Advanced event parsing** window, in the **Use raw event** drop-down list, select **Yes**.

   cef

   This parsing method is used to process CEF data.

   If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**.

regexp

This parsing method is used to create custom rules for processing data in a format using regular expressions.

You must add a regular expression (RE2 syntax) with named capturing groups to the field under **Normalization**. The name of the capturing group and its value are considered the field and value of the raw event that can be converted to an event field in KUMA format.

To add event handling rules:

1. If necessary, copy an example of the data you want to process to the **Event examples** field. We recommend completing this step.

   You can also generate regular expressions based on added examples by clicking the **Generate regular expression with KIRA** button. This automatically adds generated regular expressions to the **Normalization** group of settings.

2. In the field under **Normalization**, add a regular expression with named capture groups following the RE2 syntax, for example `"(?P<name>regexp)"`. The regular expression added to the field under **Normalization** must exactly match the event. When designing the regular expression, we recommend using special characters that match the starting and ending positions of the text: `^`, `$`.

   You can add multiple regular expressions or remove regular expressions. To add a regular expression, click **Add regular expression**. To remove a regular expression, click the delete icon ✕ next to it.

3. Click the **Copy field names to the mapping table** button.

   Capture group names are displayed in the **KUMA field** column of the **Mapping** table. You can select the corresponding KUMA field in the column opposite each capturing group. If you followed the CEF format when naming the capturing groups, you can use automatic CEF mapping by selecting the **Use CEF syntax for normalization** check box.

Event handling rules are added.

syslog

This parsing method is used to process data in syslog format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**.

To parse events in rfc5424 format with a `structured-data` section, in the **Keep extra fields** drop-down list, select **Yes**. This makes the values from the `structured-data` section available in the `Extra` fields.

csv

This parsing method is used to create custom rules for processing CSV data.

When choosing this parsing method, you must specify the separator of values in the string in the **Delimiter** field. Any single-byte ASCII character can be used as a delimiter for values in a string.

kv

This parsing method is used to process data in key-value pair format. Available parsing method settings are listed in the table below.

Available parsing method settings

Setting	Description
Pair delimiter	The character used to separate key-value pairs. You can specify any single-character (1 byte) value. The specified value must not match the value specified in the **Value delimiter** field.
Value delimiter	The character used to separate a key from its value. You can specify any single-character (1 byte) value. The specified value must not match the value specified in the **Pair delimiter** field.

xml

This parsing method is used to process XML data in which each object, including nested objects, occupies a single line in a file. Files are processed line by line.

If you want to send the raw event for advanced normalization, at each nesting level in the **Advanced event parsing** window, in the **Use raw event** drop-down list, select **Yes**.

If you select this parsing method, under **XML attributes**, you can specify the key XML attributes to be extracted from tags. If an XML structure has multiple XML attributes with different values in the same tag, you can identify the necessary value by specifying the key of the value in the **Source** column of the **Mapping** table.

To add key XML attributes:

1. Click **+ Add field**.

2. This opens a window; in that window, specify the path to the XML attribute.

You can add multiple XML attributes or remove XML attributes. To remove an individual XML attribute, click the delete icon ✕ next to it. To remove all XML attributes, click **Reset**.

If XML key attributes are not specified, then in the course of field mapping the unique path to the XML value will be represented by a sequence of tags.

Tag numbering

Starting with KUMA 2.1.3, you can use automatic tag numbering in XML events. This lets you parse an event with the identical tags or unnamed tags, such as `<Data>`.

As an example, we will number the tags of the `EventData` attribute of the Microsoft Windows PowerShell event ID 800.

View Microsoft Windows PowerShell events, event ID 800

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
        <System>
                <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-
8497-1e730c959516}" EventSourceName="NTDS" />
                <EventID Qualifiers="0000">0000</EventID>
                <Version>@</Version>
                <Level>4</Level>
                <Task>15</Task>
                <Opcode>0</Opcode>
                <Keywords >0x8080000000000000</Keywords>
                <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
                <EventRecordID>55647</EventRecordID>
                <Correlation />
                <Execution ProcessID="1" ThreadID="1" />
                <Channel>service</Channel>
                <Computer>computer</Computer>
                <Security UserID="0000" />
```

```
        </System>
        <EventData>
                <Data>583</Data>
                <Data>36</Data>
                <Data>192.168.0.1:5084</Data>
                <Data>level</Data>
                <Data>name, lDAPDisplayName</Data>
                <Data />
                <Data>5545</Data>
                <Data>3</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>15</Data>
                <Data>none</Data>
        </EventData>
</Event>
```

To parse events with identical tags or unnamed tags, you need to configure tag numbering and data mapping for numbered tags with KUMA event fields.

KUMA 3.0.x supports using XML attributes and tag numbering at the same time in the same extra normalizer. If an XML attribute contains unnamed tags or identical tags, we recommend using tag numbering. If the XML attribute contains only named tags, we recommend using XML attributes.

To use XML attributes and tag numbering in extra normalizers, you must sequentially enable the **Use raw event** setting in each extra normalizer along the path that the event follows to the target extra normalizer, and in the target extra normalizer itself.

For an example of how tag numbering works, you can refer to the **MicrosoftProducts** normalizer. The **Use raw event** setting is enabled sequentially in both **AD FS** and **424** extra normalizers.

To set up the parsing of events with unnamed or identical tags:

1. Open an existing normalizer or create a new normalizer.

2. In the **Basic event parsing** window of the normalizer, in the **Parsing method** drop-down list, select **xml**.

3. In the **Tag numbering** field, click **+ Add field**.

4. In the displayed field, enter the full path to the tag to whose elements you want to assign a number, for example, `Event.EventData.Data`. The first tag gets number 0. If the tag is empty, for example, `<Data />`, it is also assigned a number.

5. To configure data mapping, under **Mapping**, click **+ Add row** and do the following:

   a. In the displayed row, in the **Source** field, enter the full path to the tag and the index of the tag. For example, for the Microsoft Windows PowerShell event ID 800 from the example above, the full paths to tags and tag indices are as follows:

      - `Event.EventData.Data.0`
      - `Event.EventData.Data.1`
      - `Event.EventData.Data.2`

   b. In the **KUMA field** drop-down list, select the field in the KUMA event that will receive the value from the numbered tag after parsing.

6. Save changes in one of the following ways:

   - If you created a new normalizer, click **Save**.
   - If you edited an existing normalizer, in the collector to which the normalizer is linked, click **Update configuration**.

   Parsing is configured.

netflow

This parsing method is used to process data in all supported NetFlow protocol formats: NetFlow v5, NetFlow v9, and IPFIX.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. This takes into account the source fields of all NetFlow versions (NetFlow v5, NetFlow v9, and IPFIX).

If the **netflow** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

netflow5

This parsing method is used to process data in the NetFlow v5 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **netflow5** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow5** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

netflow9

This parsing method is used to process data in the NetFlow v9 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **netflow9** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **netflow9** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

sflow5

This parsing method is used to process data in sflow5 format.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **sflow5** parsing method is selected for the main parsing, extra normalization is not available.

ipfix

This parsing method is used to process IPFIX data.

If you select this parsing method, you can use the predefined rules for converting events to the KUMA format by clicking **Apply default mapping**. If the **ipfix** parsing method is selected for the main parsing, extra normalization is not available.

> The default mapping rules for the **ipfix** parsing method do not specify the protocol type in KUMA event fields. When parsing data in NetFlow format, on the **Enrichment** normalizer tab, you must create a **constant** data enrichment rule that adds the `netflow` value to the `DeviceProduct` target field.

sql

The normalizer uses this parsing method to process data obtained by making a selection from the database.

normalizer

This parsing method allows you to reuse a previously created normalizer as the primary or extra normalizer for processing events.

If you select this parsing method, in the **Normalizer** drop-down list, you need to select one of the previously created normalizers of the json, cef, regexp, syslog, csv, kv, xml, or sql type. Normalizers with the **normalizer** parsing method cannot be selected.

5. Select tags for the normalizer from the **Tags** drop-down list.

6. In the **Keep raw event** drop-down list, specify whether you want to store the original raw event in the re-created normalized event.

   - **Don't save**—do not save the raw event. This value is selected by default.

   - **Only errors**—save the raw event in the `Raw` field of the normalized event if errors occurred when parsing it. You can use this value to debug the service. In this case, an event having a non-empty `Raw` field will indicate problems.

   - **Always**—always save the raw event in the `Raw` field of the normalized event.

7. In the **Keep extra fields** drop-down list, choose whether you want to store the raw event fields in the normalized event if no mapping is configured for them (see step 8 of these instructions):

   - **No**. This value is selected by default.

   - **Yes**. The original event fields are saved in the `Extra` field of the normalized event.

   This field is not available if the **Parsing method** is set to **normalizer**.

8. If necessary, provide an example of the data you want to process to the **Event examples** field. We recommend completing this step.

   This field is not available if the **Parsing method** is set to **normalizer**.

You can add multiple event examples. Every new example must be specified on a new line. At the same time, in the **Mapping** table, its parsing result will be displayed in the **Examples** column. This lets you check whether the fields of different types of incoming events are mapped correctly.

Limitations involved in parsing event examples

When parsing the examples of data specified in the **Event examples** field, the following parameters are not taken into account in the extra normalizer:

- Enrichment configured in the root normalizer
- Filters specified in the extra normalizer
- The **Use raw event** setting
- Conversions in the root normalizer
- Conversions for the value of the **Field to pass into normalizer** parameter.

9. In the **Mapping** settings block, configure the mapping of raw event fields to KUMA event fields:

> The **Mapping** table is not available if the **Parsing method** is set to **normalizer**.

a. Click **+ Add row**.

   You can add multiple table rows or delete table rows. To delete a table row, select the check box next to it and click the **Delete** button.

b. In the **Source** column, specify the name of the raw event field that you want to map to the KUMA event field.

   For details about the field name format, refer to the Normalized event data model article. For a description of the mapping, refer to the Mapping fields of predefined normalizers article.

   If you want to create rules for modifying the fields of the original event before writing to the KUMA event fields, click the settings (⚙) icon next to the field name to open the **Conversion** window, and in that window, click **+ Add conversion**. You can reorder the rules or delete the rules. To reorder rules, use the reorder (⠿) icons. To delete a rule, click the delete (✕) icon next to it.

   Available conversions

   Conversions are modifications that are applied to a value before it is written to the event field.

   You can select one of the following conversion types from the drop-down list:

   - **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.
   - **lower**—is used to make all characters of the value lowercase
   - **upper**—is used to make all characters of the value uppercase
   - **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.
- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

c. In the **KUMA field** column, select a KUMA event field from the drop-down list. You can find the KUMA event field by typing its name. If the name of the KUMA event field begins with `DeviceCustom*` or `Flex*`, enter a unique custom label in the **Label** field, if necessary.

If you want KUMA to enrich events with asset information, and the asset information to be available in the alert card when a correlation rule is triggered, in the **Mapping** table, configure a mapping of host address and host name fields depending on the purpose of the asset. For example, you can configure a mapping for **SourceAddress** and **SourceHostName**, or **DestinationAddress** and **DestinationHostName** KUMA event fields. As a result of enrichment, the event card includes a **SourceAssetID** or **DestinationAssetID** KUMA event field, and a link to the asset card. As a result of enrichment, asset information is also available in the alert card.

If you have loaded data into the **Event examples** field, the table will have an **Examples** column containing examples of values carried over from the raw event field to the KUMA event field.

10. To add data to the created normalized events, create enrichment rules in the normalizer as follows:

a. Go the **Enrichment** tab.

The **Enrichment** tab is not available if on the **Normalization scheme** tab, the **Parsing method** is set to **normalizer**.

b. Click the **+ Add enrichment** button.

The enrichment rule settings section is displayed. You can add multiple enrichment rules or delete enrichment rules. To delete an enrichment rule, click the delete (✕) icon next to it.

c. Select an enrichment source type from the **Data source type** drop-down list. When you select some enrichment source types, additional settings may become available that you must specify.

Available Enrichment rule source types:

constant

This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "constant"

Setting	Description
Constant	The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed.
Target field	The event field to insert the data into.

If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field.

If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array.

dictionary

This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dictionary"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.

If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`.

If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`.

table

This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "table"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.
Mapping	Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`).

The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field.

If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

event

This type of enrichment is used when you need to write a value from another event field to the current event field. Available enrichment type settings are listed in the table below.

Available enrichment type settings

Setting	Description
Target field	The KUMA event field that you want to populate with the data.
Source field	The event field whose value is written to the target field.

If you want to create a rule for modifying the raw data before writing to KUMA event fields, under **Conversion**, click the **+ Add conversion** button. In the **Type** drop-down list, select a conversion type. You can add multiple conversion by clicking the **+ Add conversion** button. To delete an added conversion, click the trashcan icon next to it.

Available conversions

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

- **lower**—is used to make all characters of the value lowercase

- **upper**—is used to make all characters of the value uppercase

- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:

  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.

  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

When using enrichment of events that have **event**selected as the **Source kind** and the extended event schema fields are used as arguments, the following special considerations apply:

- If the source extended event schema field has the `Array of strings` type, and the target extended event schema field has the `String` type, the values are written to the target extended event schema field in TSV format.

  Example: the `SA.StringArray` extended event schema field contains values: `"string1"`, `"string2"`, `"string3"`. An event enrichment operation is performed. The result of the event enrichment operation is written to the `DeviceCustomString1` extended event schema field. The `DeviceCustomString1` extended event schema field contains values: `["string1", "string2", "string3"]`.

- If the source and target extended event schema fields have the `Array of strings` type, values of the source extended event schema field are added to the values of the target extended event schema field, and the `","` character is used as the delimiter.

  Example: The `SA.StringArrayOne` field of the extended event scheme contains the `["string1", "string2", "string3"]` values, and the `SA.StringArrayTwo` field of the extended event scheme contains the `["string4", "string5", "string6"]` values. An event enrichment operation is performed. The result of the event enrichment operation is written to the `SA.StringArrayTwo` field of the extended event scheme. The `SA.StringArrayTwo` extended event schema field contains values: `["string4", "string5", "string6", "string1", "string2", "string3"]`.

template

This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

d. In the **Target field** drop-down list, select the KUMA event field to which you want to write the data. You cannot select a value if in the **Source kind** drop-down list, you selected **table**.

e. If you want to enable details in the normalizer log, enable the **Debug** toggle switch. The toggle switch is turned off by default.

f. If you want to add multiple enrichment rules with different data source types, click the + **Add enrichment** button and manage the settings.

   You can reorder and delete created rules. To change the position of a rule, click ⠿ next to it. To delete a rule, click ✕ next to it.

11. Click **OK**.

12. If you want to configure additional event parsing:

    a. Hover over the dark circle and click the plus sign that appears.

    b. On the **Extra normalization conditions** tab, manage the following settings:

        a. If you want to send a raw event for extra normalization, in the **Use raw event** drop-down list, select **Yes**.

        The default value is **No**. We recommend passing a raw event to normalizers of **json** and **xml** types.

        You also need to select the **Yes** value if you want to pass a raw event for extra normalization to the second, third, and deeper nesting levels, one nesting level at a time.

        The **Use raw event** option is not applicable if the sql parsing method is used in the main event parsing rule.

        b. If you want to send for additional parsing only events with fields specified in normalizer settings, specify the raw event fields that you want to pass to the extra normalizer in the **Field to pass into normalizer** field.

        If this field is blank, the full event is sent to the extra normalizer for processing.

        If, when configuring the additional normalizer, you set the **Use raw event** setting to **No**, and left the **Source field** blank, any conversions configured for the field that is passed to the normalizer will not work. For conversions to be performed correctly, the source field must be filled, or the **Use raw event** setting must be set to Use raw event.

        KUMA does not limit or check the text that you specify in this setting.

        c. Under **Filter settings** section, configure the filtering conditions that events entering the normalizer must satisfy.

        You can use the **Add condition** button to add a string containing fields for identifying the condition (see below). You can use the **Add group** button to add a group of filters. Group operators can be switched between **AND**, **OR**, and **NOT**. You can add other condition groups and individual conditions to filter groups.

        You can swap conditions and condition groups by dragging them by the ⠿ icon; you can also delete them using the ✕ icon.

        Filter condition settings:

        - **Left operand** and **Right operand**—used to specify the values to be processed by the operator.

          In the left operand, you must specify the source field of events coming into the normalizer. For example, if the eventType - DeviceEventClass mapping is configured in the **Basic event parsing** window, then in the **Additional event parsing** window on the **Extra normalization conditions** tab, you must specify eventType in the left operand field of the filter.

          Data is processed only as text strings. KUMA does not limit or check the text that you specify in the left and right operand fields.

        - Operators:

          = – full match of the left and right operands.

          startsWith – the left operand starts with the characters specified in the right operand.

          endsWith – the left operand ends with the characters specified in the right operand.

          match – the left operand matches the regular expression (RE2) specified in the right operand.

          in – the left operand matches one of the values specified in the right operand.

The incoming data can be converted by clicking the button. This opens the **Conversion** window, in which you can click the **Add conversion** button to create the rules for converting the source data before any actions are performed on them. In the **Conversion** window, you can swap the added rules by dragging them by the icon; you can also delete them using the icon.

Available conversions

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

- **lower**—is used to make all characters of the value lowercase

- **upper**—is used to make all characters of the value uppercase

- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:
  - **decodeHexString**—used to convert a HEX string to text.
  - **decodeBase64String**—used to convert a Base64 string to text.
  - **decodeBase64URLString**—used to convert a Base64url string to text.
  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

d. Go to the **Normalization scheme** tab and manage the settings as described in steps 2–9 of these instructions.

e. Go to the **Enrichment** tab and manage the settings as described in step 10 of these instructions.

f. Click **OK**.

13. Click the **Create** button.

In the upper right corner, in the search field, you can search for additional parsing rules by name.

For normalizer resources, you can enable the display of control characters in all input fields except the **Description** field.

If, when changing the settings of a collector resource set, you change or delete conversions in a normalizer connected to it, the edits will not be saved, and the normalizer itself may be corrupted. If you need to modify conversions in a normalizer that is already part of a service, the changes must be made directly to the normalizer under **Resources** → **Normalizers** in the web interface.

Generating regular expressions with KIRA

You can automatically create one or more regular expressions based on examples of events for the normalizer with the **regexp** parsing method with the help of Kaspersky Investigation and Response Assistant. This functionality is available to users with the General Administrator, Tenant Administrator, Tier 2 Analyst, Tier 1 Analyst, and Junior Analyst roles.

To generate regular expressions:

1. Get a license with the AI module and activate the functionality in KUMA.
2. Configure the KIRA integration in one of the following ways:
   - Using Kaspersky Security Network (**KSN** mode)
   - Using a third-party LLM provider (**Custom** mode).
3. Start creating a normalizer or open the settings of an existing normalizer.
4. On the **Normalization scheme** tab, in the **Parsing method** drop-down list, select **regexp**.
5. In the **Event examples** field, add one or more example events from which you want to create a regular expression.

   You can add up to 10 one-liner events.
6. Click the **Generate regular expression with KIRA** button.
7. Confirm your request.

   After the request is processed, a window is displayed with the following information:

   - The number of tokens remaining (if you have configured integration with KIRA using KSN)
   - The number of tokens spent on the generation
   - Generated regular expressions with color highlighting of groups and corresponding snippets of example events.

   Each generated regular expression starts with the (?:ai)? group of characters.

   In the window with the created expressions, you can edit and copy the regular expression and apply the generation result by clicking the **Apply** button.

   > If the generation of the regular expression fails or does not produce the expected result, this may mean that the provider's model that you used was unable to correctly identify the components of the event or generate the regular expression. Try to start generation again. If the error recurs, add more similar examples to the **Event examples** field and restart the generation. When starting generation after an error, no additional tokens are spent.

After applying the result, the generated regular expression is automatically added to the **Normalization** field. If multiple regular expressions have been generated, the appropriate number of fields is automatically generated for each expression. Regular expressions are added in the order in which they are generated, which you can change if necessary by dragging the expressions around by the ⠿ icon.

8. After applying the generated regular expressions, save the normalizer settings by clicking the **OK** button and then the **Save** button.

Configuring extra normalization of events

Events of various formats can simultaneously occur in the same Syslog source, having different `PROCID` field values in the Syslog header.

Depending on the `PROCID`, the structure of the `message` field content may be different.

Example:

- `PROCID = application-A` means that the event contains a message in CEF format.
- `PROCID = application-B` means that the event contains a JSON message.

Given that the structure of the `message` field is different, it is necessary to configure extra normalization, which will automatically determine the format of the event and apply the appropriate parsing method.

To configure extra normalization for events, follow the steps below:

1 Creating the primary normalizer

The primary normalizer accepts all incoming Syslog events and performs basic normalization of fields.

To create a primary normalizer:

1. In the web interface, go to **Resources** → **Normalizers** and click the **Create** button.
2. In the **Name** field, enter a unique name for the normalizer. Maximum length of the name: 128 Unicode characters.
3. In the **Tenant** drop-down list, select the tenant to which the normalizer belongs.
4. In the **Parsing method** drop-down list, select **syslog**.
5. In the **Keep raw event** drop-down list, select **Never**.
6. Under **Mapping**, click **Apply default mapping**.
7. Click **OK**.

2 Creating a CEF extra normalizer

1. In the window with the created normalizer, hover over the dark circle and click the plus sign that appears.
2. On the **Extra normalization conditions** tab, in the **Use raw event** drop-down list, select **No**.
3. In the **Filter parameters** section, click the **Add condition** button and manage the filtering conditions:

   a. For the left operand, enter:

   ```
   PROCID
   ```

   b. Select **=** as the operator.

   c. For the right operand, enter:

   ```
   application-A
   ```

4. Go to the **Normalization scheme** tab.
5. In the **Name** field, enter:

   ```
   cef
   ```

6. In the **Parsing method** drop-down list, select **cef**.
7. Under **Mapping**, click **Apply default mapping**.
8. Click **OK**.

Events with `PROCID = application-A` are sent to the CEF parser and normalized to the KUMA model.

3 Creating a JSON extra normalizer

1. In the window with the created normalizer, hover over the dark circle and click the plus sign that appears.
2. On the **Extra normalization conditions** tab, in the **Use raw event** drop-down list, select **No**.
3. In the **Filter parameters** section, click the **Add condition** button and manage the filtering conditions:

   a. For the left operand, enter:

   ```
   PROCID
   ```

   b. Select **=** as the operator.

c. For the right operand, enter:

```
application-B
```

4. Go to the **Normalization scheme** tab.

5. In the **Name** field, enter:

```
json
```

6. In the **Parsing method** drop-down list, select **json**.

7. Under **Mapping**, click **Apply default mapping**.

8. Click **OK**.

Events with `PROCID = application-B` are sent to the JSON parser and normalized to the KUMA model.

4 Testing extra normalization

After configuring the extra normalizers, we recommend testing whether you have configured event routing and processing correctly.

Check the following:

- Events with `PROCID = application-A` are sent to the **CEF** extra normalizer.
- Events with `PROCID = application-B` are sent to the **JSON** extra normalizer.
- After processing, both types of events are normalized to fit the KUMA data model.

Send test events to KUMA that match each of the configured conditions and make sure that they are successfully normalized.

Expected result:

- CEF events are processed by the **cef** parser.
- JSON events are processed by the **json** parser.
- Normalized events are displayed in the **Events** section and contain fields that are mapped to the KUMA schema.

Reusing normalizers

Some of the predefined KUMA normalizers, such as **[OOTB] Apache Access file**, **[OOTB] Nginx regexp**, **[OOTB] BIND file** and **[OOTB] Squid access.log file**, are designed to handle events from log files. If the same events are received via the Syslog protocol, the message additionally contains the Syslog header, which must be processed before the message content can be parsed.

To avoid creating a separate normalizer for each method of receiving events, you can configure cascade normalization. In this case, the header is first processed using the preset **[OOTB] Syslog header** normalizer, after which the event is passed to the appropriate OOTB normalizer to parse the message content. This lets you use the same normalizer regardless of how the events are received.

To configure cascade normalization:

1. In the KUMA web interface, open the **Resources** → **Collectors** section.
2. In the list of available collectors, find and select the predefined **[OOTB] Apache Access file** collector.
3. In the displayed window, go to the **Event parsing** section and on the **Parsing flowcharts** tab, click the **Add event parsing** button.
4. On the **Normalization scheme** tab, in the **Normalizer** drop-down list, select **[OOTB] Syslog header**.
5. Click **OK**.
6. In the window with the added normalizer, hover over the dark circle and click the plus sign that appears to add an extra normalizer.
7. In the displayed window, go to the **Normalization scheme** tab.
8. In the **Parsing method** drop-down list, select **normalizer**.
9. In the **Normalizer** drop-down list, select **[OOTB] Apache Access file**.
10. Click **OK**.
11. Save the collector settings.
12. Repeat steps 2 through 11 to configure the **[OOTB] Nginx regexp**, **[OOTB] BIND file**, and **[OOTB] Squid access.log file** collectors, adding the appropriate OOTB normalizer as an extra normalizer.

After completing the configuration, make sure that events received via Syslog are subjected to both stages of normalization in sequence:

- The **[OOTB] Syslog header** extracts the Syslog header fields.
- The OOTB normalizer of the corresponding log type parses the contents of the message and ensures that the event conforms to the KUMA data model.

You can view the processing result in the KUMA web interface in the **Events** section.

Using an extended event scheme for normalization

Events coming from sources may include data that do not fit into the set of CEF event format fields. The six additional `DeviceCustomString` fields that the CEF format already provides may not be sufficient for mapping such data. For this reason, KUMA lets you create additional fields, which are called *extended event schema fields*. You can use the extended event schema fields to map the fields of the received event. Such a configuration allows saving the non-standard data in the normalized event.

You can use the extended event schema fields in normalizers for normalizing events and in other KUMA resources, for example, as widget fields, in SQL queries for filtering and searching events, in the table of events, or in presets .

You can view the list of all extended event schema fields that exist in KUMA in the **Extended fields set** section.

Recommendations and limitations

Using many unique fields of the extended event schema can reduce the performance of the system, increase the amount of disk space required for storing events, and make the information difficult to understand.

If you want to minimize the load on the storage server when searching events, preparing reports, and performing other operations on events in storage, use KUMA event schema fields as your first preference, extended event schema fields as your second preference, and the `Extra` fields as your last resort.

When using extended event schema fields, the general limit for the maximum size of an event that can be processed by the collector is the same, 4 MB.

Types

Extended event schema fields are strongly typed as shown in the table below.

Type	Availability in the normalizer	Data type
`S`	All types	String.
`N`	All types	Number.
`F`	All types	Floating point number.
`SA`	KV, JSON	Array of strings. The order of the array elements is the same as the order of the elements of the raw event.
`NA`	KV, JSON	Array of integers. The order of the array elements is the same as the order of the elements of the raw event.
`FA`	KV, JSON	Array of floats. The order of the array elements is the same as the order of the elements of the raw event.

If the data in the fields of the raw event does not match the type of the KUMA field, the value is not saved during the normalization of events if type conversion cannot be performed. For example, the string `test` cannot be written to the `DeviceCustomNumber1` KUMA field of the Number type.

Service and custom extended event schema fields

In addition to custom fields that you can add yourself, the extended event schema has service fields are reserved by KUMA. You cannot normalize custom data to the service fields. You cannot edit, delete, export, or disable service fields. All extended event schema fields with the `KL_` prefix are service fields and can be managed only from Kaspersky servers. We do not recommend using the `KL_` prefix when adding new extended event schema fields.

By default, the following service extended event schema fields are automatically added to KUMA:

- `KL_EventRoute`, type `S` for storing information about the route of the event.

  You can use this field in normalizers, as a key or value in active lists, in enrichment rules, as a query field in data collection and analysis rules, in correlation rules. You cannot use this field to detect event sources.

- `KL_AI_DLLHijackingCheckResult` , type `N` for storing the check result of a dynamic link library that can potentially be used in DLL Hijacking attacks. The result of the check is provided by the KSN service.

- The following fields are added to a correlation event:

  - `KL_CorrelationRulePriority`, type `N`
  - `KL_SourceAssetDisplayName`, type `S`
  - `KL_DestinationAssetDisplayName`, type `S`
  - `KL_DeviceAssetDisplayName`, type `S`
  - `KL_SourceAccountDisplayName`, type `S`
  - `KL_DestinationAccountDisplayName`, type `S`

  You cannot use this service fields to search for events.

Using extended event schema fields

Configuring data normalization in an extended event schema field involves the following steps:

1. **Adding an extended event schema field**

   If a field of your received event cannot be normalized to one of the CEF event format fields, including the six additional DeviceCustomString fields, add a new extended event schema field.

2. **Mapping fields in the normalizer**

   Map the raw event field to the new extended event schema field:

   1. Open an existing normalizer or create a new normalizer.
   2. Specify the basic settings of the normalizer.
   3. In the **Mapping** settings block, click **Add string** button.
   4. For the **Source** setting, enter the name of the source field in the raw event.
   5. For the **KUMA field** setting, start typing the name of the extended event schema field and select the relevant field from the drop-down list.

      The extended event schema fields in the drop-down list have names in the `<type>.<field name>` format.
   6. Click the **Save** button to save the event normalizer.

The raw event field is normalized to the selected extended event schema field.

Viewing the table of extended event schema fields

You can view the list of all extended event schema fields that exist in KUMA in the **Settings** → **Other** → **Extended event schema fields** section. The list of extended event schema fields is the same for all tenants.

Only users with the General administrator, Tenant administrator, Tier 2 analyst, Tier 1 analyst, Junior analyst, Read shared resources, and Manage shared resources roles can view the table of extended event schema fields.

The **Extended event schema fields** table contains the following information:

- **Type**—Data type of the extended event schema field.

  Possible data types:

Type	Availability in the normalizer	Data type
S	All types	String.
N	All types	Number.
F	All types	Floating point number.
SA	KV, JSON	Array of strings. The order of the array elements is the same as the order of the elements of the raw event.
NA	KV, JSON	Array of integers. The order of the array elements is the same as the order of the elements of the raw event.
FA	KV, JSON	Array of floats. The order of the array elements is the same as the order of the elements of the raw event.

- **Field name**—Name of the extended event schema field, without a type.

  You can click the name to edit the settings of the extended event schema field.

- **Status**—Whether the extended event schema field can be used in resources.

  You can **Enable** or **Disable** the toggle switch to allow or forbid using this extended event schema field in new resources. However, a disabled field is still used in resource configurations that are already operational, until you manually remove the field from the configuration; the field also remains available in the list of table columns in the **Events** section for managing old events.

  Only a user with the General administrator role can disable an extended event schema field.

- **Updated at**—Date and time of the last modification of the extended event schema field.

- **Created by**—Name of the user that created the extended event schema field.

- **Dependencies**—Number of KUMA resources, dashboard layouts, reports, presets, and field sets for searching event sources that use the extended event schema field.

  You can click the number to open a pane with a table of all resources and other KUMA entities that are using this field. For each dependency, the table displays the name, tenant (only for resources), and type. Dependencies in the table are sorted by name. Clicking the name of a dependency takes you to its page (except for dashboard layouts, presets, and saved user queries).

  You can view the dependencies of an extended event schema field only for resources and entities to whose tenants you have access. If you do not have access to the tenant, its resources are not displayed in the table, but still count towards the number of dependencies.

- **Description**—Text description of the field.

By default, the table of extended event schema fields is sorted by update date in descending order. If necessary, you can sort the table by clicking a column heading and selecting **Ascending** or **Descending**; you can also use context search by field name.

Adding, modifying, and deleting fields of the extended event schema

Users with the General administrator, Tenant administrator, Tier 2 analyst, Tier 1 analyst, Junior analyst, Manage shared resources roles can add new and edit existing extended event schema fields. Only users with the General administrator role can delete fields.

Adding fields

To add an extended event schema field:

1. In the web interface, go to **Settings** → **Other** → **Extended event schema fields** and click the **Add** button.

2. Enable or disable the **Status** toggle switch to enable or disable this extended event schema field for resources.

   The toggle switch is enabled by default. A disabled field remains available in the list of table columns in the **Events** section for managing old events.

3. In the **Type** field, select the data type of the extended event schema field.

   Possible data types

Type	Availability in the normalizer	Data type
S	All types	String.
N	All types	Number.
F	All types	Floating point number.
SA	KV, JSON	Array of strings. The order of the array elements is the same as the order of the elements of the raw event.
NA	KV, JSON	Array of integers. The order of the array elements is the same as the order of the elements of the raw event.
FA	KV, JSON	Array of floats. The order of the array elements is the same as the order of the elements of the raw event.

4. In the **Field name**, specify the name of the extended event schema field.

   Consider the following when naming extended event schema fields:

   - The name must be unique within the KUMA instance.
   - Names are case-sensitive. For example, `Field_name` and `field_name` are different names.
   - You can use Latin, Cyrillic characters and numerals. Spaces or " ~ ` @ # $ % ^ & * ( ) + - [ ] { } | \ | / . " < > ; ! , : ? = characters are not allowed.
   - If you want to use the extended event schema fields to search for event sources, you can only use Latin characters and numerals.
   - The maximum length is 128 characters.

5. If necessary, in the **Description** field, enter a description for the extended event schema field.

   We recommend describing the purpose of the extended event schema field. Only Unicode characters are allowed in the description. The maximum length is 256 characters.

6. Click the **Save** button.

A new extended event schema field is added and displayed at the top of the table. An audit event is generated for the creation of the extended event schema field. If you have enabled the field, you can use it in normalizers and when configuring resources.

Modifying fields

To edit an extended event schema field:

1. In the web interface, in the **Settings** → **Other** → **Extended event schema fields** section, click the name of the field that you want to edit.

   This opens the **Update extended field** pane. This pane displays the settings of the selected field, as well as the **Dependencies** table with a list of resources, dashboard layouts, reports, presets, and sets of fields for finding event sources that use this field. Only resources to whose tenants you have access are displayed. If the field is used by resources to whose tenant you do not have access, such resources are not displayed in the table.

   Clicking the name of a resource or entity takes you to its page (except for dashboard resources, presets, and saved user queries).

2. Make the changes you need in the available settings.

   You can edit the **Type** and **Field name** settings only if the extended event schema field does not have dependencies. You can edit the **Status** and **Description** settings for any extended event scheme field. However, a field with the **Disabled** status is still used in resource configurations that are already operational, until you manually remove the field from the configuration; the field also remains available in the list of table columns in the **Events** section for managing old events.

   Disabling an extended event schema field using the **Status** toggle switch requires the General administrator role.

3. Click the **Save** button.

The extended event schema field is updated. An audit event is generated about the modification of the field.

Deleting fields

You can delete only those extended event schema fields that are not service fields, that have the **Disabled** status, and that are not used in KUMA resources and other entities (do not have dependencies). We recommend deleting extended event schema fields after enough time has passed to make sure that all events in which the field was used have been deleted from KUMA. When you delete a field, it is no longer displayed in event tips.

To delete extended event schema fields:

1. In the web interface, go to the **Settings** → **Other** → **Extended event schema fields** section.

2. Select the check boxes in the first column of the table next to one or more fields that you want to delete.

   To select all fields, you can select the check box in the heading of the first column.

3. Click the **Delete** button in the upper part of the table.

   The **Delete** button is active only if all selected fields are disabled and have no dependencies. If at least one field is enabled or has a dependency, the button is inactive.

If you want to delete a field that is used in at least one KUMA resource, but you do not have access to its tenant, the **Delete** button is active when this field is selected. However, an error is displayed when you attempt to delete the field.

The selected fields are deleted. An audit event is generated about the deletion of the fields.

Importing and exporting extended event schema fields

You can add multiple new extended event schema fields at once by importing them from a JSON file. You can also export all extended event schema fields with information about them to a file, for example, to propagate the list of fields to other KUMA instances to maintain resources.

Users with the General administrator, Tenant administrator, Tier 2 analyst, Tier 1 analyst, Junior analyst, and Manage shared resources roles can import an export extended event schema fields. Users with the Read shared resources role can only export extended event schema fields.

To import extended event schema fields into KUMA from a file:

1. In the web interface, go to **Settings** → **Other** → **Extended event schema fields** and click the **Import** button.

2. This opens a window; in that window, select a JSON file with a list of extended event schema field objects.

Example JSON file

```
[
{"kind": "SA",
"name": "<fieldName1>",
"description": "<description1>",
"disabled": false},
{"kind": "N",
"name": "<fieldName2>",
"description": "<description2>",
"disabled": false},
....
{"kind": "FA",
"name": "<fieldNameX>",
"description": "<descriptionX>",
"disabled": false}
]
```

When importing fields from a file, their names are checked for possible conflicts with fields of the same type. If a field with the same name and type already exists in KUMA, such fields are not imported from the file.

Extended event schema fields are imported from the file to KUMA. An audit event about the import of fields is generated, and a separate audit event is generated for each added field.

To export extended event schema fields to a file:

1. In the web interface, go to the **Settings** → **Other** → **Extended event schema fields** section.

2. Do one of the following:

   - If you want to export specific extended event schema fields:

     a. Select the check boxes in the first column of the table for the required fields. You cannot select service fields.

     b. Click the **Export selected** button in the upper part of the table.

   - If you want to export all extended event schema fields, click the **Export all** button in the upper part of the table.

A JSON file with a list of extended event schema field objects and information about them is downloaded.

Using a connector

Connectors are used for establishing connections between Kaspersky SIEM services and for active and passive receiving of events.

Some connector types (such as tcp, sql, wmi, wec, and etw) support TLS encryption. The solution supports TLS 1.2 and 1.3. When TLS mode is enabled for these connectors, the connection is established according to the following algorithm:

- If Kaspersky SIEM is used as a client:

  1. The solution sends a connection request to the server with a ClientHello message specifying the maximum supported TLS version (1.3), as well as a list of supported ciphersuites.

  2. The server responds with the preferred TLS version and a ciphersuite.

  3. Depending on the TLS version in the server response:

     - If the server responds to the request with TLS 1.3 or 1.2, KUMA establishes a connection with the server.

     - If the server responds to the request with TLS 1.1, KUMA terminates the connection with the server.

- If the solution is used as a server:

  1. The client sends a connection request to KUMA with the maximum supported TLS version, as well as a list of supported ciphersuites.

  2. Depending on the TLS version in the client request:

     - If the ClientHello message of the client request specifies TLS 1.1, KUMA terminates the connection.

     - If the client request specifies TLS 1.2 or 1.3, KUMA responds to the request with the preferred TLS version and a ciphersuite.

To create a connector:

1. In the solution web interface, go to **Resources** → **Connectors**, and click the **Create** button.

2. In the **Type** drop-down list, select the connector type and specify its settings on the **Basic settings** and **Advanced settings** tabs:

   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - 1c-log
   - 1c-xml
   - diode
   - ftp
   - sftp
   - nfs
   - wmi
   - wec
   - etw
   - snmp
   - snmp-trap
   - kata/edr
   - vmware
   - elastic

- office365
- dfi
- universalAPI
- smb
- http-streaming

3. Click the **Create** button.

Connector settings

This section describes the settings of all connector types supported by KUMA.

You can view the settings of the created connectors in the **Resources** → **Connectors** section by selecting the relevant connector from the list.

Connector, internal type

Connectors of the **internal** type are mainly used to receive events from an agent to the collector via the 'internal' protocol.

A connector of this type is also used to receive the following data:

- Internal data, such as event routes.
- File attributes. If during collector creation you specified a file type connector at the Installation Wizard's Transport step, then at the **Event parsing** step in the **Mapping** table you can pass the name of the file processed by the collector or the path to the file in the KUMA event field. To do this, in the **Source** column, specify one of the following values:

  - `$kuma_fileSourceName` to pass the name of the file being processed by the collector in the KUMA event field.
  - `$kuma_fileSourcePath` to pass the path to the file being processed by the collector in the KUMA event field.

  When you use a **file** connector, the new variables in the normalizer will only work with destinations of the internal type.

- Events to the event router. The event router can only receive events over the 'internal' protocol, therefore you can only use **internal** destinations when sending events to the event router.

Settings for a connector of the **internal** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **internal**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	The URL and port that the connector is listening on. You can enter a value in one of the following formats: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Only one URL can be added. The resource or service cannot be saved if the value of the field contains spaces or tab characters. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Connector, tcp type

Connectors of the **tcp** type are used for passively receiving events over TCP when working with Windows and Linux agents. Settings for a connector of the **tcp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **tcp**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL that you want to connect to. You can enter a URL in one of the following formats: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` • `:< port number >` Required setting.

Setting	Description

Auditd	This toggle switch enables the auditd mechanism to group auditd event lines received from the connector into an auditd event.
	If you enable this toggle switch, you cannot select a value in the **Delimiter** drop-down list because **\n** is automatically selected for the mechanism.
	If you enable this toggle switch in the connector settings of the agent, you need to select **\n** in the **Delimiter** drop-down list in the cor settings of the collector to which the agent sends events.
	
	The maximum size of a grouped auditd event is approximately 4,174,304 characters.
	
	KUMA classifies Auditd events according to an algorithm. For example, suppose the following records were received for processing:
	`type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty=`
	`old-ses=4294967295 ses=2348 res=1`
	`type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a0`
	`a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)`
	`comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)`
	`type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66`
	The algorithm gives one single-line event of the LOGIN type (because the LOGIN type has code 1006 and it is less than 1300, which is AUDIT_FIRST_EVENT), and one multi-line event with SYSCALL and PROCTITLE.
	When grouping a multi-line auditd event containing records with different prefixes, the resulting event uses the prefix of the record th first. This is necessary for the normalizer to parse the event correctly. For example, suppose the following records were received for p
	`<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE`
	`msg=audit(1742441361.524:787467):`
	`proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F78`
	`<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR`
	`msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000`
	`<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.52`
	`arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid=1`
	`pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses=`
	`comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<`
	
	The `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)` r arrived first, therefore the resulting event uses the `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit` prefix.
	
	When grouping events, the solution ignores strings of the `EOE` type (for example, `type=EOE msg=audit(1633859647.072:120613)` they do not convey information that is important for the events.

Delimiter	• **\n** (used by default) • **\t** • **\0**
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Character encoding	Character encoding. The default is **UTF-8**.

Parameter	Description
Event Buffer TTL	Buffer lifetime for auditd event lines, in milliseconds. Auditd event lines enter the KUMA collector and accumulate in the buffer. This allows multiple auditd event lines to be grouped into a single auditd event. The buffer lifetime countdown begins when the first auditd event line is received or when the previous buffer lifetime expires. Possible values: from 50 to 30,000. The default value is `2000`. This field is available if you have enabled the **Auditd** toggle switch on the **Basic settings** tab. The auditd event lines accumulated in the buffer are kept in the RAM of the server. We recommend caution when increasing the buffer size because memory usage by the KUMA collector may become excessive. You can verify how much server RAM the KUMA collector is using in KUMA metrics. If you want a buffer lifetime to exceed 30,000 milliseconds, we recommend using a different auditd event transport. For example, you can use an agent or pre-accumulate auditd events in a file, and then process this file with the KUMA collector.
Transport header	Regular expression for auditd events, which is used to identify auditd event lines. You can use the default value or edit it. The regular expression must contain the `record_type_name`, `record_type_value`, and `event_sequence_number` groups. If a multi-line auditd event contains a prefix, the prefix is retained for the first line of the auditd event and discarded for the following lines. You can revert to the default regular expression for auditd events by clicking **Reset to default value**.
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the Basic settings. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified. • **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the PFX secret drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and is displayed in the **PFX secret** drop-down list. • **Custom PFX with client authentication** means TLS encryption with a PFX secret. In this mode, the client is authenticated using a certificate. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the PFX secret drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and displayed in the **PFX secret** drop-down list.

Parameter	Description
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

Connector, udp type

Connectors of the **udp** type are used for passively receiving events over UDP when working with Windows and Linux agents. Settings for a connector of the **udp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **udp**. Required setting.
URL	URL that you want to connect to. You can enter a URL in one of the following formats: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` • `:< port number >` Required setting.

Setting	Description

Auditd	This toggle switch enables the auditd mechanism to group auditd event lines received from the connector into an auditd event.
	If you enable this toggle switch, you cannot select a value in the **Delimiter** drop-down list because **\n** is automatically selected for the mechanism.
	If you enable this toggle switch in the connector settings of the agent, you need to select **\n** in the **Delimiter** drop-down list in the cor settings of the collector to which the agent sends events.
	
	The maximum size of a grouped auditd event is approximately 4,174,304 characters.
	
	KUMA classifies Auditd events according to an algorithm. For example, suppose the following records were received for processing:
	`type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty=`
	`old-ses=4294967295 ses=2348 res=1`
	`type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a0`
	`a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)`
	`comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)`
	`type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66`
	The algorithm gives one single-line event of the LOGIN type (because the LOGIN type has code 1006 and it is less than 1300, which is AUDIT_FIRST_EVENT), and one multi-line event with SYSCALL and PROCTITLE.
	When grouping a multi-line auditd event containing records with different prefixes, the resulting event uses the prefix of the record th first. This is necessary for the normalizer to parse the event correctly. For example, suppose the following records were received for p
	`<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE`
	`msg=audit(1742441361.524:787467):`
	`proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F78`
	`<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR`
	`msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000`
	`<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.52`
	`arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid=1`
	`pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses=`
	`comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<`
	
	The `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)` r arrived first, therefore the resulting event uses the `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit` prefix.
	
	When grouping events, the solution ignores strings of the `EOE` type (for example, `type=EOE msg=audit(1633859647.072:120613)` they do not convey information that is important for the events.

Delimiter	The character that marks the boundary between events: • \n • \t • \0 If you do not select a value in this drop-down list, an empty value is selected by default. This means that the connector does not parse into many, but instead passes it to the normalizer as it is.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Character encoding	Character encoding. The default is **UTF-8**.

Parameter	Description
Event Buffer TTL	Buffer lifetime for auditd event lines, in milliseconds. Auditd event lines enter the KUMA collector and accumulate in the buffer. This allows multiple auditd event lines to be grouped into a single auditd event. The buffer lifetime countdown begins when the first auditd event line is received or when the previous buffer lifetime expires. Possible values: from 50 to 30,000. The default value is `2000`. This field is available if you have enabled the **Auditd** toggle switch on the **Basic settings** tab. The auditd event lines accumulated in the buffer are kept in the RAM of the server. We recommend caution when increasing the buffer size because memory usage by the KUMA collector may become excessive. You can verify how much server RAM the KUMA collector is using in KUMA metrics. If you want a buffer lifetime to exceed 30,000 milliseconds, we recommend using a different auditd event transport. For example, you can use an agent or pre-accumulate auditd events in a file, and then process this file with the KUMA collector.
Transport header	Regular expression for auditd events, which is used to identify auditd event lines. You can use the default value or edit it. The regular expression must contain the `record_type_name`, `record_type_value`, and `event_sequence_number` groups. If a multi-line auditd event contains a prefix, the prefix is retained for the first line of the auditd event and discarded for the following lines. You can revert to the default regular expression for auditd events by clicking **Reset to default value**.
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

Connector, netflow type

Connectors of the **netflow** type are used for passively receiving events in the NetFlow format. Settings for a connector of the **netflow** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **netflow**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, sflow type

Connectors of the **sflow** type are used for passively receiving events in the sFlow format. For sFlow, only structures described in sFlow version 5 are supported.

In KUMA 4.6, additional normalization is available for events received in sFlow format.

Settings for a connector of the **sflow** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **sflow**. Required setting.
URL	URL that you want to connect to. You can enter a URL in one of the following formats: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` • `:< port number >` Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, nats-jetstream type

Connectors of the **nats-jetstream** type are used for interacting with a NATS message broker when working with Windows and Linux agents. Settings for a connector of the **nats-jetstream** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **nats-jetstream**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Authorization	Type of authorization when connecting to the URL specified in the **URL** field: • **Disabled**. This value is selected by default. • **Plain**. Authorization of this type is performed using the SASL/PLAIN mechanism, which transmits the user name and password in plain text. Typically, TLS is used to provide transmission security (encryption) in SASL/PLAIN. If this option is selected, in the **Secret** drop-down list, specify the secret containing user account credentials for authorization when connecting to the destination. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list.
Subject	The topic of NATS messages. Characters are entered in Unicode encoding. Required setting.
GroupID.	The value of the `GroupID` parameter for NATS messages. Maximum length of the value: 255 Unicode characters. The default value is `default`.

Setting	Description
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Character encoding	Character encoding. The default is **UTF-8**.

Parameter	Description

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.
	• **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the **PFX secret** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a PFX secret?
	To create a PFX secret:
	1. In the **Name** field, enter the name of the PFX secret.
	2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key.
	3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard.
	4. Then click the **Create** button.
	The PFX secret is created and displayed in the **PFX secret** drop-down list.
	The **Custom PFX** mode is not displayed when **Authorization** is set to **Plain**.

Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

Connector, kafka type

Connectors of the **kafka** type are used for communicating with the Apache Kafka data bus when working with Windows and Linux agents. Settings for a connector of the **kafka** type are described in the following tables.

Using a connector of the **kafka** type, KUMA can receive events in uncompressed as well as compressed form. Compression is performed using the following compression algorithms supported by **kafka**: gzip, snappy, zstd, or lz4. Events arriving in a compressed form are decompressed automatically.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **kafka**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.

Setting	Description
Authorization	Type of authorization when connecting to the URL specified in the **URL** field: • **Disabled**. This value is selected by default. • **Plain**. Authorization of this type is performed using the SASL/PLAIN mechanism, which transmits the user name and password in plain text. Typically, TLS is used to provide transmission security (encryption) in SASL/PLAIN. If this option is selected, in the **Secret** drop-down list, specify the secret containing user account credentials for authorization when connecting to the destination. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. • **PFX** means TLS encryption with a PFX secret. You must generate a certificate with a private key in PKCS#12 container format in an external Certificate Authority, export the PFX file from the key store, and upload the PFX file to the KUMA web interface as a PFX secret. If you select this value, in the **PFX secret** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and is displayed in the **PFX secret** drop-down list. If you are using a chain of several certificates to authenticate the server, we recommend building the PFX file using OpenSSL to ensure the correct order of certificates in the chain. • **SCRAM-SHA-256** for authorization using a secure connection mechanism that uses the SHA256 hash for secure authentication and prevents data interception. • **SCRAM-SHA-512** for authorization using a secure connection mechanism that uses the SHA512 hash for secure authentication and prevents data interception. When **SCRAM-SHA-256** or **SCRAM-SHA-512** is selected as the authorization type in the **Secret** drop-down list, specify a secret with a password for authorization. You can select an existing secret or create a new secret. To create a new secret, in the **Secret** drop-down list, select **Create new**.
Topic	Subject of Kafka messages. The maximum length of a message is 255 characters. Space and tab characters are not allowed. You can use the following characters: a–z, A–Z, 0–9, ".", "_", "-". Required setting.
GroupID.	The value of the `GroupID` parameter for Kafka messages. The maximum length of the value is 255 characters. You can use the following characters: a–z, A–Z, 0–9, ".", "_", and "-".
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999. By default, the number of handlers is 256.
Character encoding	Character encoding. The default is **UTF-8**.

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.

Size of message to fetch	Size of one message in the request, in bytes. The default value of 16 MB is applied if no value is specified or 0 is specified. It cannot exceed 2147483647 bytes.
Maximum fetch wait time	Timeout for one message in seconds. The default value of 5 seconds is applied if no value is specified or 0 is specified. Maximum possible value: 2147483647.
Connection timeout	Kafka broker connection timeout in seconds. Maximum possible value: 2147483647. The default value is 30 seconds.
Read timeout	Read operation timeout in seconds. Maximum possible value: 2147483647. The default value is 30 seconds.
Write timeout	Write operation timeout in seconds. Maximum possible value: 2147483647. The default value is 30 seconds.
Group heartbeat interval	Group status update interval in seconds. The update interval cannot exceed the session time. The recommended value is 1/3 of the session time. Maximum possible value: 2147483647. The default value is 3 seconds.

Parameter	Description
Session timeout	The session time in seconds. Maximum possible value: 2147483647. The default value is 10 seconds.
Max processing time	Maximum duration of processing one message by a single thread, in milliseconds. Maximum possible value: 2147483647. The default value is 100 milliseconds.
Auto commit enabled	Enabled by default.
Auto commit interval	Autocommit interval in seconds. The default value is 1 second. Maximum possible value: 18446744073709551615. Any positive number can be specified.

Connector, http type

Connectors of the **http** type are used for receiving events over HTTP when working with Windows and Linux agents. Settings for a connector of the **http** type are described in the following tables.

Using a connector of the **http** type, KUMA can receive events in uncompressed as well as compressed form. Events arriving in a compressed form, for example, Kaspersky Endpoint Security for Windows events, are decompressed automatically.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **http**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL that you want to connect to. You can enter a URL in one of the following formats: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` • `:< port number >` For data from the event source to be sent to the connector, the specified URL must end with `/input`. Required setting.
Delimiter	The character that marks the boundary between events: • `\n` • `\t` • `\0` If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the Basic settings. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified. • **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the PFX secret drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select Create new. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and is displayed in the **PFX secret** drop-down list. • **Custom PFX with client authentication** means TLS encryption with a PFX secret. In this mode, the client is authenticated using a certificate. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the PFX secret drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select Create new. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and displayed in the **PFX secret** drop-down list.

Connector, sql type

Connectors of the **sql** type are used for querying databases. KUMA supports multiple types of databases.

Supported database types

The solution supports the following types of SQL databases:

- SQLite.
- MariaDB 10.5 or later.
- MSSQL.

- MySQL 5.7 or later.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.

When creating a connector of the **sql** type, you must specify general connector settings and individual database connection settings. Settings for a connector of the **sql** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **sql**. Required setting.
Tags	Tags for resource search. Optional setting.
Default query	SQL query that is executed when connecting to the database. Required setting.
Reconnect to DB each time the request is sent	This toggle enables reconnection of the connector to the database every time a query is sent. This toggle switch is turned off by default.
Poll interval, sec	Interval for executing SQL queries in seconds. The default value is 10 seconds.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Connection</td><td>
Settings in this group depend on the selected database type for the connection:
MySQL
MSSQL
Postgres
SQLite3
Oracle
Firebird
ClickHouse
ODBC

Database kind is the type of the database to connect to. When you select a database type, the prefix corresponding to the communication protocol is displayed in the URL field. For example, for a ClickHouse database, the URL field contains the <code>clickhouse://</code> prefix.
The Secret separately check box allows viewing the connection information. If you selected the Secret separately check box, the credentials are specified in the Secret field, and the connection string is entered in the URL field without specifying the user's credentials.
URL is the connection URL. If you have selected the Secret separately check box, you can specify a URL without user credentials (user name and password), and then specify these credentials in a separate Secret field. If the Secret separately check box is not selected, in this field, you need to select the urls secret, inside which you need to specify the connection URL along with the user credentials (user name and password).
When creating connections, if connection information is specified in a urls secret, strings with credentials containing special characters may not be handled correctly. If an error occurs when creating a connection, but you are sure that the specified settings are correct, enter the special characters in percent encoding.
Codes of special characters
<table>
<tr><td>!</td><td>#</td><td>$</td><td>%</td><td>&</td><td>'</td><td>(</td><td>)</td><td>*</td><td>+</td></tr>
<tr><td>%21</td><td>%23</td><td>%24</td><td>%25</td><td>%26</td><td>%27</td><td>%28</td><td>%29</td><td>%2A</td><td>%2B</td></tr>
<tr><td>,</td><td>/</td><td>:</td><td>;</td><td>=</td><td>?</td><td>@</td><td>[</td><td>]</td><td>\</td></tr>
<tr><td>%2C</td><td>%2F</td><td>%3A</td><td>%3B</td><td>%3D</td><td>%3F</td><td>%40</td><td>%5B</td><td>%5D</td><td>%5C</td></tr>
</table>
<table>
<tr><td>The following special characters are not supported in passwords used to access SQL databases: space, [,], :, /, #, %, \.</td></tr>
</table>
If you selected the Secret separately check box, using any special character codes is not necessary.
If you want to edit the settings of an existing URL, click the pencil icon next to it.

Secret is a credentials secret that stores a list of URLs for connecting to the database. This field is displayed if the Secret separately check box is selected.
Identity column is the name of the column that contains the ID for each row of the table.
Required setting.
Identity seed is the value in the identity column for determining the row from which you want to start reading data from the SQL table.
Query is the additional SQL query that is executed instead of the default SQL query.
Poll interval, sec is the SQL query execution interval in seconds. The specified interval is used instead of the default interval for the connector. The default value is 10 seconds.

You can add multiple connections or delete a connection. To add a connection, click the + Add connection button. To remove a connection, click the delete ✕ icon next to it.
</td></tr>
<tr><td>Description</td><td>Description of the resource. The maximum length of the description is 4000 Unicode characters.</td></tr>
</table>

Advanced settings tab

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Debug</td><td>The switch enables resource logging. The toggle switch is turned off by default.</td></tr>
<tr><td>Character encoding</td><td>
Character encoding. The default is UTF-8.
<table>
<tr><td>KUMA converts SQL responses to UTF-8 encoding. You can configure the SQL server to send responses in UTF-8 encoding or change the encoding of incoming messages on the KUMA side.</td></tr>
</table>
</td></tr>
</table>

Within a single connector, you can **create a connection** for multiple supported databases. If a collector with a connector of the **sql** type cannot be started, check if the /opt/kaspersky/kuma/collector/<`collector ID`>/sql/state-<`file ID`> state file is empty. If the state file is empty, delete it and restart the collector.

To create a connection for multiple SQL databases:

1. Click the **Add connection** button.
2. Specify the **URL**, **Identity column**, **Identity seed**, **Query**, and **Poll interval, sec** values.
3. Repeat steps 1–2 for each required connection.

Supported SQL types and their specific usage features

The following SQL types are supported:

- MSSQL.

  For example:

  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}`

  We recommend using this URL variant.

  - `sqlserver://{user}:{password}@{server}?database={database}`

  The characters `@p1` are used as a placeholder in the SQL query.

  > If you want to connect using domain account credentials, specify the account name in `< domain >%5C< user >` format. For example: `sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`.

- MySQL/MariaDB

  For example:

  `mysql://{user}:{password}@tcp({server}:{port})/{database}`

  The characters `?` are used as placeholders in the SQL query.

- PostgreSQL.

  For example: `postgres://{user}:{password}@{server}/{database}?sslmode=disable`

  The characters `$1` are used as a placeholder in the SQL query.

- CockroachDB

  For example:

  `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`

  The characters `$1` are used as a placeholder in the SQL query.

- SQLite3

  For example:

  `sqlite3://file:{file_path}`

  A question mark (`?`) is used as a placeholder in the SQL query.

  When querying SQLite3, if the initial value of the ID is in datetime format, you must add a date conversion with the `sqlite datetime` function to the SQL query. For example:

```
select * from connections where datetime(login_time) > datetime(?, 'utc') order by login_time
```

In this example, `connections` is the SQLite table, and the value of the variable `?` is taken from the **Identity seed** field, and it must be specified in the `{< date >}T{< time >}Z` format, for example, `2021-01-01T00:10:00Z)`.

- Oracle DB

  Example URL of a secret with the 'oracle' driver:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}
  ```

  ```
  oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}
  ```

  If the query execution time exceeds 30 seconds, the oracle driver aborts the SQL request, and the following error appears in the collector log: **user requested cancel of current operation**. To increase the execution time of an SQL query, specify the value of the **timeout** parameter in seconds in the connection string, for example:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}?timeout=300
  ```

  The `:val` variable is used as a placeholder in the SQL query.

  When querying Oracle DB, if the identity seed is in the datetime format, you must consider the type of the field in the database and, if necessary, add conversions of the time string in the SQL query to make sure the SQL connector works correctly. For example, if the `Connections` table in the database has a `login_time` field, the following conversions are possible:

  - If the **login_time** field has the TIMESTAMP type, then depending on the configuration of the database, the **login_time** field may contain a value in the `YYYY-MM-DD HH24:MI:SS` format, for example, `2021-01-01 00:00:00`. In this case, you need to specify `2021-01-01T00:00:00Z` in the **Identity seed** field, and in the SQL query, perform the conversion using the `to_timestamp` function, for example:

    ```
    select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-DD"T"HH24:MI:SS"Z"')
    ```

  - If the **login_time** field has the TIMESTAMP WITH TIME ZONE type, then depending on the configuration of the database, the **login_time** field may contain a value in the `YYYY-MM-DD"T"HH24:MI:SSTZH:TZM` format (for example, `2021-01-01T00:00:00+03:00`). In this case, you need to specify `2021-01-01T00:00:00+03:00` in the Identity seed field, and in the SQL query, perform the conversion using the `to_timestamp_tz` function, for example:

    ```
    select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')
    ```

    For details about the `to_timestamp` and `to_timestamp_tz` functions, please refer to the official Oracle documentation.

  To interact with Oracle DB, you must install the libaio1 Astra Linux package.

- Firebird® SQL

  For example:

  ```
  firebirdsql://{user}:{password}@{server}:{port}/{database}
  ```

  A question mark (`?`) is used as a placeholder in the SQL query.

  If a problem occurs when connecting Firebird on Windows, use the full path to the database file, for example:

  ```
  firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB
  ```

- ClickHouse

  For example:

`clickhouse://{user}:{password}@{server}:{port}/{database}`

A question mark (`?`) is used as a placeholder in the SQL query.

KUMA supports the following data types:

- Data that can be cast to string (such as strings, numeric values, and BLOBs) is displayed as strings.
- Arrays and maps are displayed in JSON format or using the built-in `go fmt.Sprintf("%v",v)` function to display them in the best possible way.

Two methods of connecting to ClickHouse are possible:

- Without credentials, by entering a URL: `clickhouse://host:port/database`
- With credentials, by entering a URL: `clickhouse://user:password@host:port/database`

When using TLS encryption, by default, the connector works only on port 9440. If TLS encryption is not used, by default, the connector works with ClickHouse only on port 9000.

> The connector does not work over HTTP.

If TLS encryption mode is configured on the ClickHouse server, and in connector settings, in the **TLS mode** drop-down list, you have selected **Disabled** or vice versa, the database connection cannot be established.

> The **TLS mode** is used only if the ClickHouse driver is specified.

If you want to connect to the KUMA ClickHouse, in the **SQL** connector settings, specify the **PublicPKI** secret type, which contains the base64-encoded PEM private key and the public key.

In the parameters of the **SQL** connector for the ClickHouse connection type, you need to select **Disabled** in the **TLS mode** drop-down list. This value must not be specified if a certificate is used for authentication. If in the **TLS mode** drop-down list, you select **Custom CA**, you need to specify the ID of a secret of the 'certificate' type in the **Secret** field. You also need to select one of the following values in the **Authorization type** drop-down list:

- **Disabled**. If you select this value, you need to leave the **Secret** field blank.
- **Plain**. Select this value if the **Secret separately** check box is selected and the ID of a secret of the 'credentials' type is specified in the **Secret** field.
- **PublicPKI**. Select this value if the **Secret separately** check box is selected and the ID of a secret of the PublicPKI type is specified in the **Secret** field.

If the initial value of the ID contains an indication of time (`datetime`), in the query, you must use a variable for time conversion (`parseDateTimeBestEffort`). For example, if the time is specified as `2021-01-01 00:10:00`, the following query may be used:

```
select connections, username, host, login_time from connections where login_time >
parseDateTimeBestEffort(?) order by login_time
```

- ODBC

  For example:

  `odbc://{server}:{port}/{database}` if you selected the **Secret separately** check box when configuring the connection settings.

`odbc://{user}:{password}@{server}:{port}/{database}` if you selected the **Secret separately** check box when configuring the connection settings.

`odbc://{server}:{port}/{database}?params1=value1&params2=value2` if you need to specify all connection parameters.

A question mark (`?`) is used as a placeholder in the SQL query.

> ODBC is not supported when the collector is deployed in Kubernetes.

If you are using ODBC, you need to specify the name of the ODBC database driver for the **ODBC driver file name** setting. Then you need to save the driver file in the `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` directory.

> The solution uses version 2.3.14 of the ODBC Manager system utility to manage ODBC drivers and database connections. You need to use ODBC drivers that are compatible with this version of the system utility.

When specifying the name of the ODBC database driver, consider the following:

- If the driver has dependencies, you need to save them in the `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` or `/opt/kaspersky/kuma/collector/<uuid_of_collector>/` directory (if the driver so requires).
- This setting is case sensitive.
- When specifying paths, special characters are allowed.

```
Example of ODBC database driver name

psqlodbcw.so
```

To use an ODBC SQL connector in an existing collector, after upgrading the solution from version 4.2, you need to uninstall and then reinstall the collector. This lets you get the values of all environment variables that the ODBC connector needs to work correctly.

Example of configuring an SQL connector with an ODBC driver

To configure the connector for working with the ODBC driver (using the ODBC driver for PostgreSQL and Astra Linux as an example):

1. Check if an ODBC exists for your database. If such a driver exists, find out the file name of this driver with the .so extension by looking it up online.
2. In the **Resources** → **Connectors** section, create an SQL connector, in the **Database kind** field, select **ODBC**.
3. Fill in all the required fields for the new connector by specifying the name of the ODBC driver in the **ODBC driver file name** field.

   If necessary, you can change the name of the driver after installing the collector with the specified connector.
4. Install the collector with an SQL connector on the host.

5. Download the appropriate .so file. For PostgreSQL, you can download this file using the following command:

```
apt download odbc-postgresql
```

The solution downloads the `ibpq5_15.17-astra.se2.3r2_amd64.deb` package for Astra Linux.

6. Do the following:

   a. Unpack the `ibpq5_15.17-astra.se2.3r2_amd64.deb` package by running the following command:

   ```
   ar x libpq5_15.17-astra.se2.3r2_amd64.deb
   ```

   b. Unpack the `data.tar.xz` archive by running the following command:

   ```
   tar -xf data.tar.xz
   ```

7. Among the extracted files, find .so files by running the following command:

```
find . -name ".so"
```

8. Copy the PostgreSQL ODBC driver to the `driver` directory inside the collector directory by running the following command:

```
cp ./usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so
```

9. Verify that all ODBC driver dependencies are satisfied on the host by running the following command:

```
LD_LIBRARY_PATH="/opt/kaspersky/kuma/collector/<ID>/deps/odbc:/opt/kaspersky/kuma/collector/<ID>/driver"
ldd /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so | grep "not found"
```

where `<ID>` is the ID of the installed collector.

If the command displays `libpq.so.5 => not found`, you need to additionally download the `libpq.so.5` dependency. For Astra Linux, you can also do this by running the following command:

```
apt download libpq5
```

After that, unpack the deb package and search for the .so file. Move the .so file thus found to the `driver` directory in the collector folder (`cp ./usr/lib/x86_64-linux-gnu/libpq.so.5.15 /opt/kaspersky/kuma/collector/<ID>/driver/libpq.so.5`).

10. Recheck all ODBC driver dependencies on the host. Also, make sure that the name of the driver file in the `driver` directory of the collector (`/opt/kaspersky/kuma/` collector/<ID>/driver/psqlodbcw.so) matches the file name in the configuration file.

    To conduct diagnostics and make sure there are no missing dependencies, you can add the `-Environment=LD_DEBUG=libs` line to the systemd file of the collector and run the following command:

```
systemctl daemon-reload
```

Then restart the collector; `journalctl` will display information about the ODBC driver searching for dependencies.

Each kind of ODBC driver has its own special way of presenting information about missing dependencies. For example, the MsSQL ODBC driver looks for dependencies one level above the `driver` directory. You need to save the missing `share` folder in `/opt/kaspersky/kuma/collector/<ID>`, not in the `driver` directory. There may also be peculiarities involved in specifying the URL depending on the ODBC driver. For example, for the Oracle ODBC driver, you need to specify the URL in the connector configuration file in the following format: `odbc://?DBQ=//{server}:{port}/{database}` (in this case, the user name and password are specified in a secret of the credentials type in the **Secret** field, if you have selected the **Secret separately** check box).

> When configuring an ODBC driver, we recommend following the documentation of the specific driver.

11. Restart the collector.

A sequential request for database information is supported in SQL queries. For example, if in the **Query** field, you enter `select * from <name of data table> where id > <placeholder>`, the value of the **Identity seed** field is used as the placeholder value the first time you query the table. In addition, the service that utilizes the SQL connector saves the ID of the last read entry, and the ID of this entry will be used as the placeholder value in the next query to the database.

> We recommend adding the `order by` command to the query string, followed by the sorting field. For example, `select * from table_name where id > ? order by id`.

Examples of SQL requests

SQLite, Firebird, MySQL, MariaDB, ClickHouse, ODBC: `select * from table_name where id > ? order by id`

MSSQL: `select * from table_name where id > @p1 order by id`

PostgreSQL, Cockroach: `select * from table_name where id > $1 order by id`

Oracle: `select * from table_name where id > :val order by id`

Connector, file type

Connectors of the **file** type are used for getting data from text files when working with Windows and Linux agents. One line of a text file is considered to be one event. `\n` is used as the newline character.

If during collector creation you specified a **file** type connector at the Installation Wizard's Transport step, then at the **Event parsing** step in the **Mapping** table you can pass the name of the file processed by the collector or the path to the file in the KUMA event field. To do this, in the **Source** column, specify one of the following values:

- `$kuma_fileSourceName` to pass the name of the file being processed by the collector in the KUMA event field.
- `$kuma_fileSourcePath` to pass the path to the file being processed by the collector in the KUMA event field.

When you use a **file** connector, the new variables in the normalizer will only work with destinations of the internal type.

To read Windows files, you need to create a connector of the **file** type and manually install the agent on Windows. The Windows agent must not read its files in the folder where the agent is installed. The connector will work even with a FAT file system; if the disk is defragmented, the connector re-reads all files from scratch because all inodes of files are reset.

> We do not recommend running the agent under an administrator account; read permissions for folders/files must be configured for the user account of the agent. We do not recommend installing the agent on important systems; it is preferable to send the logs and read them on dedicated hosts with the agent.

For each file that the connector of the **file** type interacts with, a state file (states.ini) is created with the `offset`, `dev`, `inode`, and `filename` parameters. The state file allows the connector, to resume reading from the position where the connector last stopped instead of starting over when rereading the file. Some special considerations are involved in rereading files:

- If the `inode` parameter in the state file changes, the connector rereads the corresponding file from the beginning. When the file is deleting and recreated, the `inode` setting in the associated state file may remain unchanged. In this case, when rereading the file, the connector resumes reading in accordance with the `offset` parameter.
- If the file has been truncated or its size has become smaller, the connector start reading from the beginning.
- If the file has been renamed, when rereading the file, the connector resumes reading from the position where the connector last stopped.
- If the directory with the file has been remounted, when rereading the file, the connector resumes reading from the position where the connector last stopped. You can specify the path to the files with which the connector interacts when configuring the connector in the **File path** field.

Settings for a connector of the **file** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **file**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description
Path to the file.	Connectors of the **file** type are used for getting data from text files when working with Windows and Linux agents. One line of a text f considered to be one event. `\n` is used as the newline character. The full path to the file that the connector interacts with. Both Linux and Windows path formats are supported, for example: • Windows: `C:\var\log\test123.log` • Linux: `/var/log/test123.log` Paths that match the following regular expressions are not allowed: • `(?i)^[a-zA-Z]:\\Program Files` • `(?i)^[a-zA-Z]:\\Program Files\(x86\)` • `(?i)^[a-zA-Z]:\\Windows` • `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` In these regular expressions, the double backslashes (\\) are parsed by the system as part of the regular expression syntax and must n manually specified in the path itself. **File and folder mask templates** Masks: • `'*'` —matches any sequence of characters. • `'[' [ '^' ] { < range of characters > } ']'` —class of characters (may not be left blank). • `'?'` —matches any single character. Ranges of characters: • `[0-9]` for numerals • `[a-zA-Z]` for Latin alphabet characters Example: Masks can be used in both Linux and Windows paths, with backslashes replacing forward slashes as appropriate: • Linux: • `/var/log/*som?[1-9].log` • `/mnt/dns_logs/*/dns.log` • `/mnt/proxy/access*.log` • Windows: • `C:\var\log\test123.log` • `D:\data\*\report?.txt` **Limitations when using prefixes in file paths** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/`

Setting	Description

	• `/usr/local/*`
	• `/usr/local/sbin/`
	• `/usr/local/bin/`
	• `/usr/sbin/`
	• `/usr/lib/`
	• `/usr/lib64/`
	• `/var/*`
	• `/var/lib/`
	• `/var/run/`
	• `/opt/kaspersky/kuma/`
	
	These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters be manually specified in the path itself if it is not part of a valid path.
	
	Files are available at the following paths:
	
	• `/opt/kaspersky/kuma/clickhouse/logs/`
	• `/opt/kaspersky/kuma/metrics/log/`
	
	Limiting the number of files for watching by mask
	
	The number of files simultaneously watched by mask can be limited by the `max_user_watches` setting of the Core. To view the value of this setting, command:
	
	`cat /proc/sys/fs/inotify/max_user_watches`
	
	If the number of files for watching exceeds the value of the `max_user_watches` setting, the collector cannot read any more events from the files ar following error is written to the collector log:
	
	`Failed to add files for watching {"error": "no space left on device"}`
	
	To make sure that the collector continues to work correctly, you can configure the appropriate rotation of files so that the number of files does not e value of the `max_user_watches` setting, or increase the `max_user_watches` value.
	
	To increase the value of this setting, run the command:
	
	`sysctl fs.inotify.max_user_watches=< number of files >`
	
	`sysctl -p`
	
	You can also add the value of the `max_user_watches` setting to sysctl.conf so make sure it is kept indefinitely.
	
	After you increase the value of the `max_user_watches` setting, the collector resumes correct operation.
	
	Required setting.

Update timeout, sec	The time in seconds for which the file must not be updated for KUMA to apply the action specified in the **Timeout action** drop-down l file. Default value: `0`, meaning that if the file is not updated, KUMA does not apply any action to it. The entered value must not be less than the value that you entered on the **Advanced settings** in the **Poll interval, ms** field.
Timeout action	The action that KUMA applies to the file after the time specified in the **Update timeout, sec**: • **Do nothing**. The default value. • **Add suffix** adds the .kuma_processed extension to the file name and does not process the file even when it is updated. • **Delete** deletes the file.

Setting	Description
Auditd	This toggle switch enables the auditd mechanism to group auditd event lines received from the connector into an auditd event. If you enable this toggle switch, you cannot select a value in the **Delimiter** drop-down list because **\n** is automatically selected for the mechanism. If you enable this toggle switch in the connector settings of the agent, you need to select **\n** in the **Delimiter** drop-down list in the cor settings of the collector to which the agent sends events. The maximum size of a grouped auditd event is approximately 4,174,304 characters. KUMA classifies Auditd events according to an algorithm. For example, suppose the following records were received for processing: `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty= old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a0 a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` The algorithm gives one single-line event of the LOGIN type (because the LOGIN type has code 1006 and it is less than 1300, which is AUDIT_FIRST_EVENT), and one multi-line event with SYSCALL and PROCTITLE. When grouping a multi-line auditd event containing records with different prefixes, the resulting event uses the prefix of the record th first. This is necessary for the normalizer to parse the event correctly. For example, suppose the following records were received for p `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F78` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.52 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid=1 pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses= comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<`  The `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)` r arrived first, therefore the resulting event uses the `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit` prefix.  When grouping events, the solution ignores strings of the `EOE` type (for example, `type=EOE msg=audit(1633859647.072:120613)` they do not convey information that is important for the events.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
File/folder polling mode	Specifies how the connector rereads files in the directory: • **Track changes** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field if the files are not being updated. The default value. For example, if the files are constantly being updated, and the value of **Poll interval, ms** is `5000`, the connector rereads the files continuously instead of every 5000 milliseconds. If the files are not being updated, the connector rereads them every 5000 milliseconds. • **Track periodic** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field, regardless of whether the files are being updated or not.

Parameter	Description
Poll interval, ms	The interval in milliseconds at which the connector rereads files in the directory. Default value: `0` means the connector rereads files in the directory every 700 milliseconds. In the **File/folder polling mode** drop-down list, select the mode the connector must use to reread files in the directory. The entered value must not be less than the value that you entered on the **Basic settings** in the **Update timeout, sec** field. We recommend entering a value less than the value that you entered in the **Event Buffer TTL** field because this may adversely affect the performance of Auditd.
Character encoding	Character encoding. The default is **UTF-8**.
Event Buffer TTL	Buffer lifetime for auditd event lines, in milliseconds. Auditd event lines enter the KUMA collector and accumulate in the buffer. This allows multiple auditd event lines to be grouped into a single auditd event. The buffer lifetime countdown begins when the first auditd event line is received or when the previous buffer lifetime expires. Possible values: 700 to 30,000. The default value is `2000`. This field is available if you have enabled the **Auditd** toggle switch on the **Basic settings** tab. The auditd event lines accumulated in the buffer are kept in the RAM of the server. We recommend caution when increasing the buffer size because memory usage by the KUMA collector may become excessive. You can verify how much server RAM the KUMA collector is using in KUMA metrics. If you want a buffer lifetime to exceed 30,000 milliseconds, we recommend using a different auditd event transport. For example, you can use an agent or pre-accumulate auditd events in a file, and then process this file with the KUMA collector.
Transport header	Regular expression for auditd events, which is used to identify auditd event lines. You can use the default value or edit it. The regular expression must contain the `record_type_name`, `record_type_value`, and `event_sequence_number` groups. If a multi-line auditd event contains a prefix, the prefix is retained for the first line of the auditd event and discarded for the following lines. You can revert to the default regular expression for auditd events by clicking **Reset to default value**.

Connector, 1c-log type

Connectors of the **1c-log** type are used for getting data from 1C technology logs when working with Linux agents. `\n` is used as the newline character. The connector accepts only the first line from a multi-line event record.

Settings for a connector of the **1c-log** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **1c-log**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description
Directory path	The full path to the directory with the files that you want to interact with, for example, `/var/log/1c/logs/`. **Limitations when using prefixes in file paths** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path. Files are available at the following paths: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
File/folder polling mode	Specifies how the connector rereads files in the directory: • **Track changes** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field if the files are not being updated. The default value. For example, if the files are constantly being updated, and the value of **Poll interval, ms** is `5000`, the connector rereads the files continuously instead of every 5000 milliseconds. If the files are not being updated, the connector rereads them every 5000 milliseconds. • **Track periodic** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field, regardless of whether the files are being updated or not.
Poll interval, ms	The interval in milliseconds at which the connector rereads files in the directory. Default value: `0` means the connector rereads files in the directory every 700 milliseconds. In the **File/folder polling mode** drop-down list, select the mode the connector must use to reread files in the directory.
Character encoding	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.

Connector operation diagram:

1. All 1C technology log files are searched. Log file requirements:

   - Files with the LOG extension are created in the log directory (`/var/log/1c/logs/` by default) within a subdirectory for each process (click the link below to see an image).

Example of a supported 1C technology log structure

```
/var/log/1c
└── logs
    ├── ragent_1426
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── ragent_1427
    │   ├── 22121518.log
    │   ├── 22121519.log
    │   ├── 22121520.log
    │   ├── 22121521.log
    │   ├── 22121522.log
    │   ├── 22121523.log
    │   ├── 22121600.log
    │   ├── 22121601.log
    │   ├── 22121602.log
    │   ├── 22121603.log
    │   ├── 22121604.log
    │   └── 22121605.log
    ├── rmngr_1542
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── rmngr_1544
    │   ├── 22121518.log
    │   ├── 22121519.log
```

Example of a supported 1C technology log structure

- Events are logged to a file for an hour; after that, the next log file is created.
- The file names have the following format: <YY><MM><DD><HH>.log. For example, 22111418.log is a file created in 2022, in the 11th month, on the 14th at 18:00.
- Each event starts with the event time in the following format: <mm>:<ss>.<microseconds>-<duration in microseconds>.

2. The processed files are discarded. Information about processed files is stored in the file /<collector working directory>/1c_log_connector/state.json.
3. Processing of the new events starts, and the event time is converted to the RFC3339 format.
4. The next file in the queue is processed.

Connector limitations:

- Installation of a collector with a 1c-log connector is not supported in a Windows operating system. To set up transfer of 1C log files for processing by the KUMA collector:

  1. On the Windows server, grant read access over the network to the folder with the 1C log files.

  2. On the Linux server, mount the shared folder with the 1C log files on the Linux server (see the list of supported operating systems).

  3. On the Linux server, install the collector that you want to process 1C log files from the mounted shared folder.

- Only the first line from a multi-line event record is processed.

- The normalizer processes only the following types of events:

  - ADMIN
  - ATTN
  - CALL
  - CLSTR
  - CONN
  - DBMSSQL
  - DBMSSQLCONN
  - DBV8DBENG
  - EXCP
  - EXCPCNTX
  - HASP
  - LEAKS
  - LIC
  - MEM
  - PROC
  - SCALL
  - SCOM
  - SDBL
  - SESN

- SINTEG
- SRVC
- TLOCK
- TTIMEOUT
- VRSREQUEST
- VRSRESPONSE

Connector, 1c-xml type

Connectors of the **1c-xml** type are used for getting data from 1C registration logs when working with Linux agents. When the connector handles multi-line events, it converts them into single-line events.

Settings for a connector of the **1c-xml** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **1c-xml**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description
Directory path	The full path to the directory with the files that you want to interact with, for example, `/var/log/1c/logs/`. **Limitations when using prefixes in file paths** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path. Files are available at the following paths: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
File/folder polling mode	Specifies how the connector rereads files in the directory: • **Track changes** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field if the files are not being updated. The default value. For example, if the files are constantly being updated, and the value of **Poll interval, ms** is `5000`, the connector rereads the files continuously instead of every 5000 milliseconds. If the files are not being updated, the connector rereads them every 5000 milliseconds. • **Track periodic** means the connector rereads files in the directory at an interval in milliseconds specified in the **Poll interval, ms** field, regardless of whether the files are being updated or not.
Poll interval, ms	The interval in milliseconds at which the connector rereads files in the directory. Default value: `0` means the connector rereads files in the directory every 700 milliseconds. In the **File/folder polling mode** drop-down list, select the mode the connector must use to reread files in the directory.
Character encoding	Character encoding. The default is **UTF-8**.

Connector operation diagram:

1. The files containing 1C logs with the XML extension are searched within the specified directory. Logs are placed in the directory either manually or using an application written in the 1C language, for example, using the `DownloadRegistrationLog()` function. The connector only supports logs received this way. For more information on how to obtain 1C logs, see the official 1C documentation.

2. Files are sorted in ascending order of modification time. The connector saves information about the last processed file and does not process files that were modified before it. When the state is reset (for example, when an empty file is found), previously processed files can be processed again.

   Information about processed files is stored in the file `/<collector working directory>/1c_xml_connector/state.ini` and has the following format: `offset=<number>\ndev=<number>\ninode=<number>`.

3. Events are defined in each unread file.

4. Events from the file are processed one by one. Multi-line events are converted to single-line events.

Connector limitations:

- Installation of a collector with a 1c-xml connector is not supported on Windows devices. To set up transfer of 1C log files for processing by the KUMA collector:

  1. On the Windows server, grant read access over the network to the folder with the 1C log files.

  2. On the Linux server, mount the shared folder with the 1C log files on the Linux server (see the list of supported operating systems).

  3. On the Linux server, install the collector that you want to process 1C log files from the mounted shared folder.

- Files with an incorrect event format are not read. For example, if event tags in the file are in Russian, the collector does not read such events.

  Example of a correct XML file with an event

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns: v8e="http://v8.1c.ru/eventLog"
```

```
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <v8e:Event>
                <v8e:Level>Information</v8e:Level>
                <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
                <v8eApplicationName>generator.go</v8e:ApplicationName>

<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
                <v8e:Event>Test event type: Count test</v8e:Event>
                <v8e:EventPresentation></v8e:Event Presentation>
                <v8e:User>abcd_1234</v8e:User>
                <v8e:UserName>TestUser</v8e:UserName>
                <v8e:Computer>Test OC</v8e:Computer>
                <v8e:Metadata></v8e:Metadata>
                <v8e:MetadataPresentation></v8e:MetadataPresentation>
                <v8e:Comment></v8e:Comment>
                <v8e:Data>
                        <v8e:Name></v8e:Name>
                        <v8e:CurrentOSUser></v8e:CurrentOSUser>
                </v8e:Data>
                <v8e:DataPresentation></v8e:DataPresentation>
                <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
                <v8e:TransactionID></v8e:TransactionID>
                <v8e:Connection>0</v8e:Connection>
                <v8e:Session></v8e:Session>
                <v8e:ServerName>kuma-test</v8e:ServerName>
                <v8e:Port>80</v8e:Port>
                <v8e:SyncPort>0</v8e:SyncPort>
        </v8e:Event>
</v8e:EventLog>
```


Example of a processed event


```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```


Example of a processed event

- If there an empty log file (file without events) is found in the directory, the connector resets the information about the last processed file. As a result, previously processed files can be processed again. To avoid processing events twice, use one of the following approaches:
  - Use a file name mask that excludes new empty files from processing, and rename the file after the first event is written to it.
  - Before creating a new file, rename the already-processed files so that they no longer match the connector's search mask.
- If a file read by the connector is enriched with the new events and if this file is not the last file read in the directory, all events from the file are processed again.

Connector, diode type

Connectors of the **diode** type are used for unidirectional data transmission in industrial ICS networks using data diodes. Settings for a connector of the **diode** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **diode**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description
Data diode destination directory	Full path to the directory on the KUMA collector server, into which the data diode moves files with events from the isolated network segment. After the connector has read these files, the files are deleted from the directory. Maximum length of the path: 255 Unicode characters. **Limitations when using prefixes in paths** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path. Files are available at the following paths: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Required setting.

Setting	Description
Delimiter	The character that marks the boundary between events: • \n • \t • \0 If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged. You must select the same value in the **Delimiter** drop-down list in the settings of the connector and the destination being used to transmit events from the isolated network segment using a data diode.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Poll interval, sec	Interval at which the files are read from the directory containing events from the data diode. The default value is 2 seconds.
Character encoding	Character encoding. The default is **UTF-8**.
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**. You must select the same value in the **Snappy** drop-down list in the settings of the connector and the destination being used to transmit events from the isolated network segment using a data diode.

Connector, ftp type

Connectors of the **ftp** type are used for getting data over File Transfer Protocol (FTP) when working with Windows and Linux agents. Settings for a connector of the **ftp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **ftp**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description

URL	URL of file or file mask that begins with the `'ftp://'` schema. You can use `* ? [...]` for the file mask.
	File mask templates
	Masks:
	• `'*'` —matches any sequence of characters.
	• `'['` `[ '^' ]` `{ < range of characters > }` `']'` —class of characters (may not be left blank).
	• `'?'` —matches any single character.
	Ranges of characters:
	• `[0-9]` for numerals
	• `[a-zA-Z]` for Latin alphabet characters
	Example:
	Masks can be used in both Linux and Windows paths, with backslashes replacing forward slashes as appropriate:
	• Linux:
	  • `/var/log/*som?[1-9].log`
	  • `/mnt/dns_logs/*/dns.log`
	  • `/mnt/proxy/access*.log`
	• Windows:
	  • `C:\var\log\test123.log`
	  • `D:\data\*\report?.txt`
	If the URL does not contain the port number of the FTP server, port `21` is automatically specified.
	Required setting.

Secret	
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, sftp type

Connectors of the **sftp** type are used for getting data over Secure File Transfer Protocol (SFTP) when working with Windows and Linux agents.

The sftp connector gets events from files on a remote SFTP server. The connector periodically goes through the specified files by name or mask and sends any new data to the normalizer. This connector requires an SSH connection to the SFTP server.

The connector is designed for log files in which new lines are appended to the end of the file. If you clear a file, reduce its size, or change the file without changing its size, the connector will reread the entire file from the start and will re-send the events to the normalizer.

Directory poll and file read interval: 2 seconds

Buffer size: 1 MB

Settings for a connector of the **sftp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **sftp**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL of log file or file mask that begins with the `'sftp://'` schema, for example, `sftp://example.com:22/path/to/file.log`. You can use `* ? [...]` for the file mask. Masks are not allowed in directory names. KUMA gets information only from files in the final directory of the path. Suppose you specify the following path: `sftp://< host_name >:< port >/< directory_name1 >/< directory_name2 >/< mask >` In this case, KUMA will get information only from files in directory2. If directory2 has further subdirectories, files from these will not be read. **File mask templates** Masks: • `'*'` —matches any sequence of characters. • `'[' [ '^' ] { < range of characters > } ']'` —class of characters (may not be left blank). • `'?'` —matches any single character. Ranges of characters: • `[0-9]` for numerals • `[a-zA-Z]` for Latin alphabet characters Example: Masks can be used in file names in both Linux and Windows paths, with backslashes replacing forward slashes as appropriate: • Linux: • `/var/log/*som?[1-9].log` • `/mnt/proxy/access*.log` • Windows: • `C:\var\log\test123.log` • `D:\data\log\report?.txt` If the URL does not contain the port number of the SFTP server, port `22` is automatically specified. Required setting.

SSH server public keys	Public keys used to authenticate the SFTP server when establishing an SSH connection. You can specify multiple keys of different types, and the connector will automatically select the appropriate key.
	Format: `<key_type> <base64-value>`
	Example of a key: ssh-ed25519 ABCD...
	On the server, public keys are stored at the following path:
	`/etc/ssh/ssh_host_*_key.pub`
	You can also get public keys by running the following command:
	`ssh-keyscan [-p port] [-t type] [host | addrlist namelist]`
	Example commands:
	`ssh-keyscan example.com`
	`ssh-keyscan -p 2222 -t rsa,ed25519 example.com`
	Required setting.

Setting	Description
Secret	Secret that stores the credentials for connecting to the SFTP server. Secrets of the **credentials** and **ssh private key** type are supported. The secret must contain either a user name plus password or a user name plus an SSH private key. If you do not need credentials to connect to the SFTP server, leave the user name and password fields empty. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Encoding of files received from the SFTP server. The default encoding is UTF-8. Optional setting.

Connector, nfs type

Connectors of the **nfs** type are used for getting data over Network File System (NFS) when working with Windows and Linux agents. Settings for a connector of the **nfs** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **nfs**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	Path to the remote directory in the `nfs://< host name >/< path >` format. Required setting.
File name mask	A mask used to filter files containing events. The following wildcards are acceptable `"*"`, `"?"`, `"[...]"`.
Poll interval, sec	Poll interval in seconds. The time interval after which files are re-read from the remote system. The default value is `0`.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, wmi type

Connectors of the **wmi** type are used for getting data using Windows Management Instrumentation when working with Windows agents. Settings for a connector of the **wmi** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **wmi**. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.
URL	URL of the collector that you created to receive data using Windows Management Instrumentation, for example, `kuma-collector.example.com:7221`. When a collector is created, an agent is automatically created that will get data on the remote device and forward it to the collector service. If you know which server the collector service will be installed on, the URL is known in advance. You can enter the URL of the collector in the **URL** field after completing the installation wizard. To do so, you first need to copy the URL of the collector in the **Resources** → **Active services** section. Required setting.
Default credentials	In the **Remote hosts** table, you need to specify credentials for connecting to hosts that can be used by default. This field is required if the secret for at least one host is not specified in the **Remote hosts** table.

Setting	Description
Remote hosts	Settings of remote Windows devices to connect to. • **Server** is the IP address or name of the device from which you want to receive data, for example, `machine-1`. Cyrillic characters are not supported. Required setting. • **Domain** is the name of the domain in which the remote device resides, for example, `example.com`. Cyrillic characters are not supported. Required setting. • **Log type** are the names of the Windows logs that you want to get. By default, this drop-down list includes only preconfigured logs, but you can add custom log to the list. To do so, enter the names of the custom logs in the **Windows logs** field, then press **ENTER**. KUMA service and resource configurations may require additional changes in order to process custom logs correctly. Logs that are available by default: • Application • ForwardedEvents • Security • System • HardwareEvents If a WMI connection uses at least one log with an incorrect name, the agent that uses the connector does not receive events from all the logs within this connection, even if the names of other logs are specified correctly. The WMI agent connections for which all log names are specified correctly will work properly. Required setting. • In the **Secret** field, specify account credentials for accessing a remote Windows device with permissions to read the logs. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. When creating a secret, you do not need to specify the domain for accessing the host in the **User** field because the **Domain** value from the **Remote hosts** table is used. If you want to edit the settings of an existing secret, click the pencil icon. If you leave the **default** value in this field, the credentials specified in the **Default credentials** field are used when connecting to remote Windows devices. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. You can add multiple remote Windows devices or remove a remote Windows device. To add a remote Windows device, click **+ Add**. To remove a remote Windows device, select the check box next to it and click **Delete**. You can also click the **Import** button to import a file with a list of remote Windows devices in TSV format, which lets you avoid filling in fields manually when you have many such devices. KUMA automatically fills in the data from the file and performs a check. An error is displayed for incorrectly filled fields. You can edit these fields manually and save the settings.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified.

Parameter	Description
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

If you edit a connector of this type, the **TLS mode** and **Compression** settings are visible and available on the connector resource as well as the collector. If you are using a connector of this type on a collector, the values of **TLS mode** and **Compression** settings are sent to the destination of automatically created agents.

Receiving events from a remote device

Conditions for receiving events from a remote Windows device hosting a KUMA agent:

- To start the KUMA agent on the remote device, you must use an account with the "Log on as a service" permissions.
- To receive events from the KUMA agent, you must use an account with Event Log Readers permissions. For domain servers, one such user account can be created so that a group policy can be used to distribute its rights to read logs to all servers and workstations in the domain.
- TCP ports 135, 445, and 49152–65535 must be opened on the remote Windows devices.
- You must run the following services on the remote machines:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

Connector, wec type

Connectors of the **wec** type are used for getting data using Windows Event Forwarding (WEF) and Windows Event Collector (WEC), or local operating system logs of a Windows host when working with Windows agents. Settings for a connector of the **wec** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **wec**. Required setting.
Tags	Tags for resource search. Optional setting.

Setting	Description
URL	URL of the collector that you created to receive data using Windows Event Collector, for example, `kuma-collector.example.com:7221`. When a collector is created, an agent is automatically created that will get data on the remote device and forward it to the collector service. If you know which server the collector service will be installed on, the URL is known in advance. You can enter the URL of the collector in the **URL** field after completing the installation wizard. To do so, you first need to copy the URL of the collector in the **Resources** → **Active services** section. Required setting.
Windows logs	The names of the Windows logs that you want to get. By default, this drop-down list includes only preconfigured logs, but you can add custom log to the list. To do so, enter the names of the custom logs in the **Windows logs** field, then press **ENTER**. KUMA service and resource configurations may require additional changes in order to process custom logs correctly. Preconfigured logs: • Application • ForwardedEvents • Security • System • HardwareEvents If the name of at least one log is specified incorrectly, the agent using the connector does not receive events from any log, even if the names of other logs are correct. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified.
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

If you edit a connector of this type, the **TLS mode** and **Compression** settings are visible and available on the connector resource as well as the collector. If you are using a connector of this type on a collector, the values of **TLS mode** and **Compression** settings are sent to the destination of automatically created agents.

To start the KUMA agent on the remote device, you must use a service account with the "Log on as a service" permissions. To receive events from the operating system log, the service user account must also have Event Log Readers permissions.

You can create one user account with "Log on as a service" and "Event Log Readers" permissions, and then use a group policy to extend the rights of this account to read the logs to all servers and workstations in the domain.

We recommend that you disable interactive logon for the service account.

Connector, etw type

Connectors of the **etw** type are used for getting extended logs of DNS servers. Settings for a connector of the **etw** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **etw**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL of the DNS server. Required setting.
Session name	Session name that corresponds to the ETW provider: Microsoft-Windows-DNSServer {EB79061A-A566-4698-9119-3ED2807060E7}. If in a connector of the **etw** type, the session name is specified incorrectly, an incorrect provider is specified in the session, or an incorrect method is specified for sending events (to send events correctly, on the Windows Server side, you must specify "Real time" or "File and Real time" mode), events will not arrive from the agent, an error will be recorded in the agent log on Windows, and the status of the agent will be green. At the same time, no attempt will be made to get events every 60 seconds. If you modify session settings on the Windows side, you must restart the etw agent and/or the session for the changes to take effect. For details about specifying session settings on the Windows side to receive DNS server events, see the Configuring receipt of DNS server events using the ETW agent section. Required setting.
Extract event information	This toggle switch enables the extraction of the minimum set of event information that can be obtained without having to download third-party metadata from the disk. This method helps conserve CPU resources on the computer with the agent. By default, this toggle switch is enabled and all event data is extracted.
Extract event properties	This toggle switch enables the extraction of event properties. If this toggle switch is disabled, event properties are not extracted, which helps save CPU resources on the machine with the agent. By default, this toggle switch is enabled and event properties are extracted. You can enable the **Extract event properties** switch only if the **Extract event information** toggle switch is enabled.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified.

Parameter	Description
Compression	Drop-down list for configuring Snappy compression: • **Disabled**. This value is selected by default. • **Use Snappy**.

If you edit a connector of this type, the **TLS mode** and **Compression** settings are visible and available on the connector resource as well as the collector. If you are using a connector of this type on a collector, the values of **TLS mode** and **Compression** settings are sent to the destination of automatically created agents.

Connector, snmp type

Connectors of the **snmp** type are used for getting data over Simple Network Management Protocol (SNMP) when working with Windows and Linux agents. To process events received over SNMP, you must use the json normalizer. Supported SNMP protocol versions:

- snmpV1
- snmpV2
- snmpV3

Only one **snmp** connector created in the agent settings can be used in an agent. If you need to use multiple **snmp** connectors, you must create one or all **snmp** connectors as a separate resource and select it in the connection settings.

Available settings for a connector of the **snmp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **snmp**. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Setting	Description

SNMP resource	Settings for connecting to an SNMP resource:
	• **SNMP version** is the version of the SNMP protocol being used.
	Required setting.
	• **Host** is the name or IP address of the host. Possible formats:
	  • `<host name>`
	  • `<IPv4 address>`
	  • `<IPv6 address>`
	Required setting.
	• **Port** is the port number to be used when connecting to the host. Typical values are `161` or `162`.
	Required setting.
	• **Secret** is the secret that stores the credentials for connecting over the Simple Network Management Protocol. The secret type must match the SNMP version.
	You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a secret?
	To create a secret:
	1. In the **Name** field, enter the name of the secret.
	2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector.
	3. If necessary, enter a description of the secret in the **Description** field.
	4. Then click the **Create** button.
	The secret is added and displayed in the **Secret** drop-down list.
	Required setting.
	You can add multiple connections to SNMP resources or delete an SNMP resource connection. To create a connection to an SNMP resource, click the **+ SNMP resource** button. To delete a connection to an SNMP resource, click the delete icon next to the SNMP resource.

Settings	Rules for naming the received data, according to which OIDs (object identifiers) are converted to the keys with which the normalizer can interact. Available settings: • **Parameter name** is the name for the data type, for example, `Host name` or `Host uptime`. Required setting. • **OID** is a unique identifier that determines where to look for the required data at the event source, for example, `1.3.6.1.2.1.1.5`. KUMA requests data using the SNMP GET command. Required setting. • **Key** is a unique identifier returned in response to a request to the device with the value of the requested parameter, for example, `sysName`. You can reference the key when normalizing data. Required setting. • If the **MAC address** check box is selected, KUMA correctly decodes data where the OID contains information about the MAC address in OctetString format. After decoding, the MAC address is converted to a `String` value of the XX:XX:XX:XX:XX:XX format. You can do the following with rules: • Add multiple rules. To add a rule, click the **+ Add** button. • Delete rules. To delete a rule, select the check box next to it and click **Delete**. • Clear rule settings. To do so, click the **Clear all values** button.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, snmp-trap type

Connectors of the **snmp-trap** type are used for passively receiving events using SNMP traps when working with Windows and Linux agents. The connector receives snmp-trap events and prepares them for normalization by mapping SNMP object IDs to temporary keys. Then the message is passed to the JSON normalizer, where the temporary keys are mapped to the KUMA fields and an event is generated. To process events received over SNMP, you must use the json normalizer. Supported SNMP protocol versions:

- snmpV1
- snmpV2

Settings for a connector of the **snmp-trap** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **snmp-trap**. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

SNMP resource	Connection settings for receiving snmp-trap events:
	• **SNMP version** is the version of the SNMP protocol being used:
	  • **snmpV1**
	  • **snmpV2**
	  For example, Windows uses the snmpV2 version of the SNMP protocol by default.
	  Required setting.
	• **URL** is the URL for receiving SNMP trap events. You can enter a URL in one of the following formats:
	  • `< host name >:< port number >`
	  • `< IPv4 address >:< port number >`
	  • `< IPv6 address >:< port number >`
	  • `:< port number >`
	  Required setting.
	You can add multiple connections or delete a connection. To add a connection, click the **+ SNMP resource** button. To remove a SNMP resource, click the delete ✕ icon next to it.

Setting	Description
Settings	Rules for naming the received data, according to which OIDs (object identifiers) are converted to the keys with which the normalizer can interact. Available settings: • **Parameter name** is the name for the data type, for example, `Host name` or `Host uptime`. Required setting. • **OID** is a unique identifier that determines where to look for the required data at the event source, for example, `1.3.6.1.2.1.1.5`. KUMA requests data using the SNMP GET command. Required setting. • **Key** is a unique identifier returned in response to a request to the device with the value of the requested parameter, for example, `sysName`. You can reference the key when normalizing data. Required setting. • If the **MAC address** check box is selected, KUMA correctly decodes data where the OID contains information about the MAC address in OctetString format. After decoding, the MAC address is converted to a `String` value of the XX:XX:XX:XX:XX:XX format. You can do the following with rules: • Add multiple rules. To add a rule, click the **+ Add** button. • Delete rules. To delete a rule, select the check box next to it and click **Delete**. • Clear rule settings. To do so, click the **Clear all values** button. • Populate the table with mappings for OID values received in WinEventLog logs. To do this, click the **Apply OIDs for WinEventLog** button. If more data needs to be determined and normalized in the incoming events, add to the table rows containing OID objects and their keys. Data is processed according to the allow list principle: objects that are not specified in the table are not sent to the normalizer for further processing.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**. When receiving snmp-trap events from Windows with Russian localization, if you encounter invalid characters in the event, we recommend changing the character encoding in the **snmp-trap** connector to Windows 1251.

Configuring the source of SNMP trap messages for Windows

Configuring a Windows device to send SNMP trap messages to the KUMA collector involves the following steps:

1. **Configuring and starting the SNMP and SNMP trap services**
2. **Configuring the Event to Trap Translator service**

Events from the source of SNMP trap messages must be received by the KUMA collector, which uses a connector of the snmp-trap type and a json normalizer.

Configuring and starting the SNMP and SNMP trap services

To configure and start the SNMP and SNMP trap services in Windows 10:

1. Open **Settings** → **Apps** → **Apps and features** → **Optional features** → **Add feature** → **Simple Network Management Protocol (SNMP)** and click **Install**.
2. Wait for the installation to complete and restart your computer.
3. Make sure that the SNMP service is running. If any of the following services are not running, enable them:
   - **Services** → **SNMP Service**.
   - **Services** → **SNMP Trap**.

4. Right-click **Services** → **SNMP Service**, and in the context menu select **Properties**. Specify the following settings:

   - On the **Log On** tab, select the **Local System account** check box.

   - On the **Agent** tab, fill in the **Contact** (for example, specify `User-win10`) and Location (for example, specify `detroit`) fields.

   - On the **Traps** tab:

     - In the **Community Name** field, enter **community public** and click **Add to list**.

     - In the **Trap destination** field, click **Add**, specify the IP address or host of the KUMA server on which the collector that waits for SNMP events is deployed, and click **Add**.

   - On the **Security** tab:

     - Select the **Send authentication trap** check box.

     - In the **Accepted community names** table, click **Add**, enter **Community Name public** and specify **READ WRITE** as the **Community rights**.

     - Select the **Accept SNMP packets from any hosts** check box.

5. Click **Apply** and confirm your selection.

6. Right click **Services** → **SNMP Service** and select **Restart**.

To configure and start the SNMP and SNMP trap services in Windows XP:

1. Open **Start** → **Control Panel** → **Add or Remove Programs** → **Add / Remove Windows Components** → **Management and Monitoring Tools** → **Details**.

2. Select **Simple Network Management Protocol** and **WMI SNMP Provider**, and then click **OK** → **Next**.

3. Wait for the installation to complete and restart your computer.

4. Make sure that the SNMP service is running. If any of the following services are not running, enable them by setting the **Startup type** to **Automatic**:

   - **Services** → **SNMP Service**.

   - **Services** → **SNMP Trap**.

5. Right-click **Services** → **SNMP Service**, and in the context menu select **Properties**. Specify the following settings:

   - On the **Log On** tab, select the **Local System account** check box.

   - On the **Agent** tab, fill in the **Contact** (for example, specify `User-win10`) and Location (for example, specify `detroit`) fields.

- On the **Traps** tab:
  - In the **Community Name** field, enter **community public** and click **Add to list**.
  - In the **Trap destination** field, click **Add**, specify the IP address or host of the KUMA server on which the collector that waits for SNMP events is deployed, and click **Add**.
- On the **Security** tab:
  - Select the **Send authentication trap** check box.
  - In the **Accepted community names** table, click **Add**, enter **Community Name public** and specify **READ WRITE** as the **Community rights**.
  - Select the **Accept SNMP packets from any hosts** check box.

6. Click **Apply** and confirm your selection.
7. Right click **Services** → **SNMP Service** and select **Restart**.

Changing the port for the SNMP trap service

You can change the SNMP trap service port if necessary.

To change the port of the SNMP trap service:

1. Open the C:\Windows\System32\drivers\etc folder.
2. Open the **services** file in Notepad as an administrator.
3. In the **service name** section of the file, specify the snmp-trap connector port added to the KUMA collector for the **SNMP trap** service.
4. Save the file.
5. Open the Control Panel and select **Administrative Tools** → **Services**.
6. Right-click **SNMP Service** and select **Restart**.

Configuring the Event to Trap Translator service

To configure the Event to Trap Translator service that translates Windows events to SNMP trap messages:

1. In the command line, type `evntwin` and press **Enter**.
2. Under **Configuration type**, select **Custom**, and click the **Edit** button.
3. In the **Event sources** group of settings, use the **Add** button to find and add the events that you want to send to KUMA collector with the SNMP trap connector installed.
4. Click the **Settings** button, in the opened window, select the **Don't apply throttle** check box, and click **OK**.
5. Click **Apply** and confirm your selection.

Connector, kata/edr type

Connectors of the **kata/edr** type are used for getting KEDR data via the API. Settings for a connector of the **kata/edr** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **kata/edr**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Secret	Secret that stores the credentials for connecting to the KATA/EDR server. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. Required setting.
External ID	Identifier for external systems. KUMA automatically generates an ID and populates this field with it.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. We only recommend configuring a conversion if you find invalid characters in the fields of the normalized event. By default, no value is selected.
Number of events	Maximum number of events in one request. By default, the value set on the KATA/EDR server is used.

Parameter	Description
Events fetch timeout	The time in seconds to wait for receipt of events from the KATA/EDR server. Default value: `0`, which means that the value set on the KATA/EDR server is used.
Client timeout	Time in seconds to wait for a response from the KATA/EDR server. Default value: `0`, corresponding to 1800 seconds.
KEDRQL filter	Filter of requests to the KATA/EDR server. For more details on the query language, please refer to the KEDR Help.

Connector, vmware type

Connectors of the **vmware** type are used for getting VMware vCenter data via the API. Settings for a connector of the **vmware** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **vmware**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	URL of the VMware API. You need to include the hostname and port number in the URL. You can only specify one URL. Required setting.
VMware credentials	Secret that stores the user name and password for connecting to the VMware API. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. Required setting.
Sleep time, sec	Time to wait after a request that did not return events before making a new request. The default value is 5 seconds. If you specify `0`, the default value is used.
Fetch size	Number of events requested from the VMware API in one request. The default value is `100`. The maximum value is `1000`.
Start timestamp	Starting date and time from which you want to read events from the VMware API. By default, events are read from the VMware API from the time when the collector was started. If started after the collector is stopped, the events are read from the last saved date.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.

Connector, elastic type

Connectors of the **elastic** type are used for getting Elasticsearch data. Elasticsearch version 7.0.0 is supported. Settings for a connector of the **elastic** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **elastic**. Required setting.

Setting	Description
Tags	Tags for resource search. Optional setting.
Connection	Elasticsearch server connection settings: • **URL** is the URL of the Elasticsearch server. You can add multiple URLs or remove an URL. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting. • **Index name** is the name of the index in Elasticsearch. Required setting. • **Query** is the Elasticsearch query. We recommend specifying the `size` parameter in the query to prevent performance problems with KUMA and Elasticsearch, as well as the `sort` parameter for the sorting order. The following values are possible for the `sort` parameter in the query: `asc`, `desc`, or a custom sorting order by specific fields in accordance with the Elasticsearch syntax. To sort by a specific field, we recommend also specifying the `"missing" : "_first"` parameter next to the `"order"` parameter to prevent errors in cases when this field is absent in any document. For example, `"sort": { "DestinationDnsDomain.keyword": {"order": "desc", "missing" : "_first" } }`. For more details on sorting, please refer to the Elasticsearch documentation. Query example: `"query" : { "match_all" : {} }, "size" : 25, "sort": {"_doc" : "asc"}` Required setting. • **Elastic credentials** is the secret that stores the credentials for connecting to the Elasticsearch server. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. • **Elastic fingerprint** is the secret that stores secrets of the 'fingerprint' type for connecting to the Elasticsearch server and secrets of the 'certificate' type for using a CA certificate. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. • **Poll interval, sec** is the interval between queries to the Elasticsearch server in seconds if the previous query did not return any events. If Elasticsearch contained events at the time of the request, the connector will receive events until all available events have been received from Elasticsearch. You can add multiple connections to an Elasticsearch server resources or delete an Elasticsearch server connection. To add an Elasticsearch server connection, click the **+ Add connection** button. To delete an Elasticsearch server connection, click the delete ✕ icon next to the Elasticsearch server.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, office365 type

Connectors of the **office365** type are used for receiving Microsoft 365 (Office 365) data via the API.

Available settings for a connector of the **office365** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **office365**. Required setting.
Tags	Tags for resource search. Optional setting.
Office365 content types	Content types that you want to receive in KUMA. The following content types are available, providing information about actions and events in Microsoft 365, grouped by information source: • **Audit.General** • **Audit.AzureActiveDirectory** • **Audit.Exchange** • **Audit.Sharepoint** • **DLP.All** You can find detailed information about the properties of the available content types and related events in the schema on the Microsoft website. Required setting. You can select one or more content types.
Office365 tenant ID	Unique ID that you get after registering an account with Microsoft 365. If you do not have one, contact your administrator or Microsoft. Required setting.
Office365 client ID	Unique ID that you get after registering an account with Microsoft 365. If you do not have one, contact your administrator or Microsoft. Required setting.
Authorization	Authorization method for connecting to Microsoft 365. The following authorization methods are available: • **PFX**. Using a PFX secret. • **Token**. Using a 'token' secret. For more information, see the section on secrets.
Office365 credentials	The field becomes available after selecting the authorization method. You can select one of the available authorization secrets or create a new secret of the selected type. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
Authentication endpoint	The URL that is used for connection and authorization. By default, a connection is made to https://login.microsoftonline.com.
Resource endpoint	URL from which the events are to be received. The default address is https://manage.office.com.
Look back interval, hours	The period for which all new events are requested, in hours. To avoid losing some events, it is important to set overlapping event reception intervals, because some types of Microsoft 365 content may be sent with a delay. In this case, previously received events are not duplicated. By default, all new events for the last 12 hours are requested.
Request timeout, sec	Time to wait for a response to a request to get new events, in seconds. The default response timeout is 30 seconds.

Parameter	Description
Retry interval, sec	The time in seconds after which a failed request to get new events must be repeated. By default, a request to get new events is repeated 10 seconds after getting an error or no response within the specified timeout.
Clean interval, sec	How often obsolete data is deleted, in seconds. The minimum value is 300 seconds. By default, obsolete data is deleted every 1800 seconds.
Poll interval, min	How often requests for new events are sent, in minutes. By default, requests are sent every 10 minutes.
Proxy server	Proxy settings, if necessary to connect to Microsoft 365. You can select one of the available proxy servers or create a new proxy server.

Connector, dfi type

Connectors of the **dfi** are used for receiving Kaspersky Digital Footprint Intelligence data via the API. Settings for a connector of the **dfi** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **dfi**. Required setting.
Tags	Tags for resource search. Optional setting.

URL	URL of the Kaspersky Threat Intelligence Portal service API. In the URL, you need to include the hostname and port number, or just the hostname. You can only specify one URL. Kaspersky TIP address: https://tip.kaspersky.com/api.
	The following URL formats are supported:
	• `host name : port` or `host name`
	Examples:
	`http://tip_hostname:2134/api`
	`http://tip_hostname/api`
	• `IPv4 address : port` or `IPv4 address`
	Examples:
	`http://127.0.0.1:2134/api`
	`http://127.0.0.1/api`
	• `[ IPv6 address ]: port` or `[ IPv6 address ]`.
	The IPv6 address must be specified in square brackets. Examples:
	`http://[1050:0:0:0:5:600:300c:326b]:2134/api`
	`http://[1050:0:0:0:5:600:300c:326b]/api`.
	KUMA does not allow saving a resource or service if the URL field contains a tab or space character.
	Required setting.

Setting	Description
Secret	Secret that stores the credentials for connecting to the Kaspersky Threat Intelligence Portal server. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **Token** field, specify the API token for authentication on the Kaspersky Threat Intelligence Portal. You can find detailed information on getting an API token in the Kaspersky Threat Intelligence Portal Help. 3. If necessary, in the **Tags** field, add tags for the secret. 4. If necessary, enter a description of the secret in the **Description** field. 5. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. Required setting.
Poll interval	The interval in seconds between requests to the Kaspersky Digital Footprint Intelligence service. Enter a number from 60 to 3600 (that is, from 1 minute to 60 minutes). The default value is `120`. Required setting.
Start timestamp	The starting date and time for the data that the Kaspersky Digital Footprint Intelligence service generates in response to the request. By default, a request to Kaspersky Digital Footprint Intelligence is generated with data for the last 30 days up to the moment when the collector was started. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Proxy server	Proxy server settings, if one is necessary to connect to the Kaspersky Threat Intelligence Portal server. You can select one of the available proxy servers or create a new proxy server. By default, a proxy server is not used.
Character encoding	Character encoding. The default is **UTF-8**.

Connector, universalAPI type

Connectors of the **universalAPI** type are used for receiving data from any REST APIs that support JSON responses.

This connector type is designed only for REST APIs that can be configured via the user interface. Only one connection can be created for one connector. Only one URL can be configured for a connection.

For connectors of the **universalAPI** type, the **json** normalizer is usually used. However, such connectors can accept API responses not only as a JSON structure, but also as a string or number. You can use other normalizers to handle such responses, such as **regexp** or **kv**.

The **universalAPI** connector supports collecting events from JSON structures with only one nesting level. If the response structure contains nested lists (for example, a list of objects that each have another list of objects inside), the connector does not support collecting events from such lists. In this case, we recommend collecting top-level data and processing nested structures at the normalizer level.

The **universalAPI** connector does not pass empty events containing a `{}` or `[]` object to the normalizer.

You can test the connection to the source after running the collector by analyzing its logs. In case of problems with the connection or authorization issues, the collector is displayed in the **Resources** → **Active services** section with a yellow status.

> The **universalAPI** connector does not replace other existing API connectors, such as **office365**.

Settings for a connector of the **universalAPI** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **universalAPI**. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.
URL	URL of the REST API server. You do not need to specify the connection protocol (http or https). It is inferred automatically from the `tlsMode` setting. You can only specify one URL. Required setting.
Poll interval, sec	The poll interval for the specified URL, in seconds. Enter a number from `60` to `86,400` (that is, from 1 minute to 24 hours). The default value is `3600`.
HTTP method	HTTP method used for API requests. Available values: • **GET** • **POST** • **PUT** • **DELETE** Required setting.
Authorization	Authorization method for connecting to the API. The following authorization methods are available: • **Disabled**. No authorization. • **Plain**. Login and password authorization. You need to use a secret of the **credentials** type. • **Token**. Token authorization. You need to use a secret of the **token** type. For more information, see the section on secrets. The default value is **Disabled**. If on the **Advanced settings** tab, the **TLS mode** field is set to **Custom PFX**, the **Authorization** field is not available.
Secret ID	This field is available if the **Authorization** field is set to **Plain**. You need to select a secret of the **credentials** type. Required setting.
Token	This field is available if the **Authorization** field is set to **Token**. You need to select a secret of the **token** type. Required setting.
Token name	This field is available if the **Authorization** field is set to **Token**. Available values: • **Bearer** • **OAuth** You can also specify the name manually. Required setting.
Request body	The body of the HTTP request. You can also use variables: `$token`, `$username`, `$password`, `$identityValue`.

Setting	Description
Data path in JSONPath format	The data path in the structure of the API response that points to an object or a list of objects. The path is specified in JSONPath format (for example, `$.data`, `$.data.edges[0].node.event`, `$.data.edges[*].node.event`). If a string or number is expected in the API response, specify the `$` character as the path. If the **Identity field** setting is disabled, and iteration settings are not configured, data will be passed to the normalizer without changes. Required setting.
Identity field	Toggle switch for enabling a unique ID by which events will be selected. The toggle switch is turned off by default.
Path to the field in JSONPath format	This field is available if the **Identity field** toggle switch is enabled. The path to the ID field in the structure of the API response element is specified in the JSONPath format (for example, `$.id`). Required setting.
Type	This field is available if the **Identity field** toggle switch is enabled. Type of the ID field by which the events will be selected. Available values: • **int** • **float** • **string** • **date** Internally, the value is stored as a timestamp in milliseconds. Required setting.
Date format	This field is available if the **Type** field is set to **date**. The date format can include the date, time, fractions of a second, and time zone, for example, `YYYY-MM-DDTHH:mm:ssX`. The specified format is used: • For parsing the initial value of the ID. • For parsing ID values from REST API responses. If the date format does include a time zone, the value is processed in the specified time zone. If the date format does not include a time zone, the value is processed as UTC. • For generating date strings for query parameters (e.g., `$identityValue` in `queryParams`, `headers`, `body`). If the date format includes a time zone, the string is generated in the server's time zone. If the date format does not include a time zone, the string is generated as UTC.
Identity seed	This field is available if the **Identity field** toggle switch is enabled. The identity seed is specified as a string in the format corresponding to the selected **Type**. For the **date** type, you need to specify the value in the format specified in the **Date format** field. This value can contain Unicode characters. The minimum length is 1 character.
Iteration parameters	Toggle switch that enables the iteration mode used for APIs with staged data output. The toggle switch is turned off by default.
Path to the field with the iteration key in JSONPath format	The path to the iteration key field in the structure of the API response element in JSONPath format. Required setting.
Poll interval in iteration mode (sec.)	URL poll interval in iteration mode, in seconds. Maximum value: `86,400` (24 hours). The default value is `60`.
Iteration key URL parameter	Name of the URL parameter in which the iteration key is passed when making a request to the API.
Optional request parameters	Additional request parameters in the `map[string][]string` format. You can also use variables: `$token`, `$username`, `$password`, `$identityValue`. To add a parameter, click the **+ Add** button and fill in the **Key** and **Value** fields. To delete a parameter, select the check box next to it and click **Delete**. If iteration is enabled and the state has an iteration key, it is automatically substituted into the request parameters.
Request headers	Optional HTTP request headers in the `map[string][]string` format. You can also use variables: `$token`, `$username`, `$password`, `$identityValue`. To add a parameter, click the **+ Add** button and fill in the **Key** and **Value** fields. To delete a parameter, select the check box next to it and click **Delete**.
Additional fields	Additional fields are added to each data element in the `map[string][]string` format. To add fields, click the **+ Add** button and fill in the **Field name** and **JSONPath** fields. To delete a field, select the check box next to it and click **Delete**.

Advanced settings tab

Parameter	Description
Debug	Toggle switch that enables debug mode for the connector. Turned off by default.
Character encoding	Character encoding. The default is **UTF-8**.
Proxy server	Proxy settings, if necessary to connect to the API. You can select one of the available proxy servers or create a new proxy server.

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	• **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the **Custom PFX** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a PFX secret
	To create a PFX secret:
	1. In the **Name** field, enter the name of the PFX secret.
	2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key.
	3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard.
	4. Then click the **Create** button.
	The PFX secret is created and is displayed in the **PFX secret** drop-down list.

Request timeout (sec)	Time to wait for a response to an API request, in seconds. The default response timeout is 30 seconds.
Retries	The number of repeated attempts to make a request if an error occurs. The default value is `1`.
Retry interval (sec.)	Interval between retries, in seconds. The default value is `0`.

Connector, smb type

Connectors of the **smb** type are used to receive data via the SMB (Server Message Block) protocol when working with Linux agents. Available settings for a connector of the **smb** type are described in the tables below.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Connector type: **smb**. Required setting.
Tags	Tags for resource search. Optional setting.
URL	Path to the remote directory in one of the following formats: • `smb://< ip_address or host_name >:< port >/< shared_resource_name >` • `smb://< ip_address or host_name >:< port >/< shared_resource_name >/< directory_path >` KUMA gets information only from files in the final directory of the path. Suppose you specify the following path: `smb://< ip_address or host_name >:< port >/< shared_resource_name >/< directory1 >/< directory2 >` In this case, KUMA will get information only from files in directory2. If directory2 has further subdirectories, files from these will not be read. If the port is not specified, KUMA will automatically use port 445. Required setting.
File name mask	A mask used to filter files containing events. The following wildcards are acceptable "`*`", "`?`", "`[...]`". Example: *.json Required setting.
Secret	Secret that stores the credentials for connecting to the SMB server. Secrets of **credentials** type are supported. Authentication is performed using the NTLMv2 protocol. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. Required setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Debug	The switch enables resource logging. The toggle switch is turned off by default.
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. The minimum value is 16. Maximum value: 67,108,864 (64 MB). Default buffer size: 1,048,576 (1 MB); in the interface it is displayed as **Auto**.
Number of handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Poll interval, ms	Interval in milliseconds at which the connector rereads files in the directory. The default value is `0`. With this value, the connector rereads files in the directory every 700 milliseconds.
Character encoding	Encoding of files received from the SMB server. The default encoding is UTF-8. Required setting.

Predefined connectors

The KUMA distribution kit includes the predefined connectors listed in the table below.

Predefined connectors

Connector name	Comment
[OOTB] Continent SQL	Obtains events from the database of the Continent hardware and software encryption system. To use it, you must configure the settings of the corresponding secret type.
[OOTB] InfoWatch Person Monitor SQL	Collects system audit events from the MS SQL DBMS of InfoWatch Person Monitor 10.2.
[OOTB] InfoWatch Traffic Monitor SQL	Obtains events from the database of the InfoWatch Traffic Monitor system. To use it, you must configure the settings of the corresponding secret type.
[OOTB] Kaspersky Security for MS Exchange Server SQL	Collects events from the MS SQL DBMS of Kaspersky Security for Microsoft Exchange Servers version 9.0. To use it, you must configure the settings of the corresponding secret type.
[OOTB] KSC MSSQL	Obtains events from the MS SQL database of the Kaspersky Security Center system. To use it, you must configure the settings of the corresponding secret type.
[OOTB] KSC MySQL	Obtains events from the MySQL database of the Kaspersky Security Center system. To use it, you must configure the settings of the corresponding secret type.
[OOTB] KSC PostgreSQL	Obtains events from the PostgreSQL database of the Kaspersky Security Center 15.0 system. To use it, you must configure the settings of the corresponding secret type.
[OOTB] Oracle Audit Trail SQL	Obtains audit events from the Oracle database. To use it, you must configure the settings of the corresponding secret type.
[OOTB] Parsec ParsecNET MSSQL	Collects events from the MS SQL DBMS of ParsecNET 3. To use it, you must configure the settings of the corresponding secret type.
[OOTB] SecretNet SQL	Obtains events from the SecretNet SQL database. To use it, you must configure the settings of the corresponding secret type.
[OOTB] TeamPass MySQL	Collects events from the MySQL DBMS of the TeamPass system version 3.1.
[OOTB] Zabbix MySQL	Collects events from the MySQL DBMS of Zabbix version 6.4.

Using a destination

Destinations define network settings for sending normalized events. In collectors and correlators, destinations define where processed events are sent. Typically, correlators and storages act as destinations.

The following predefined destinations are included in the KUMA distribution kit and you can use them when creating a collector and a correlator:

- [OOTB] Correlator: sends events to the correlator.
- [OOTB] Storage: sends events to the storage.

To create a destination:

1. In the web interface, go to **Resources** → **Destinations** and click the **Create** button.
2. On the **Basic settings** tab, in the **Name** field, enter a unique name for the destination. The name must contain 1 to 128 Unicode characters.
3. You can use the **State** toggle switch to enable or disable the service
4. In the **Type** drop-down list, select the destination type and configure the necessary settings on the **Basic settings** and **Advanced settings** tabs, depending on the selected type:
   - internal
   - nats-jetstream
   - tcp
   - udp
   - http
   - diode
   - kafka
   - file
   - storage
   - correlator
   - eventRouter
5. Click the **Create** button.

Destination, internal type

Destinations of the **internal** type are used for receiving data from KUMA services using the 'internal' protocol. You can transfer the following data using the internal protocol:

- Internal data, such as event routes.
- File attributes. If during collector creation you specified a file type connector at the Installation Wizard's Transport step, then at the **Event parsing** step in the **Mapping** table you can pass the name of the file processed by the collector or the path to the file in the KUMA event field. To do this, in the **Source** column, specify one of the following values:
  - `$kuma_fileSourceName` to pass the name of the file being processed by the collector in the KUMA event field.
  - `$kuma_fileSourcePath` to pass the path to the file being processed by the collector in the KUMA event field.

  When you use a **file** connector, the new variables in the normalizer will only work with destinations of the **internal** type.
- Events to the event router. Destinations of the **internal** type are used to send events to the event router. The event router also has its own **eventRouter** type, which is used to configure the router accordingly.

Settings for a destination of the **internal** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **internal**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 16777216 (16 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Proxy server	The proxy server for the destination. You can select an existing proxy server or create a new proxy server. To create a new proxy server, select **Create new**. If you want to edit the settings of an existing proxy server, click the pencil icon next to it.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Health check timeout	Interval, in seconds, for checking the health of the destination.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, type nats-jetstream

Destinations of the **nats-jetstream** type are used for communication through NATS. Settings for a destination of the **nats-jetstream** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **nats-jetstream**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Subject	The topic of NATS messages. Characters are entered in Unicode encoding. Required setting.

Setting	Description
Authorization	Type of authorization when connecting to the URL specified in the **URL** field: • **Disabled**. This value is selected by default. • **Plain**. Authorization of this type is performed using the SASL/PLAIN mechanism, which transmits the user name and password in plain text. Typically, TLS is used to provide transmission security (encryption) in SASL/PLAIN. If this option is selected, in the **Secret** drop-down list, specify the secret containing user account credentials for authorization when connecting to the destination. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**

Parameter	Description

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.
	• **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the **PFX secret** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a PFX secret?
	To create a PFX secret:
	1. In the **Name** field, enter the name of the PFX secret.
	2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key.
	3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard.
	4. Then click the **Create** button.
	The PFX secret is created and displayed in the **PFX secret** drop-down list.
	The **Custom PFX** mode is not displayed when **Authorization** is set to **Plain**.

Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**.
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.

Parameter	Description
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description

Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**.
	If you want to edit the settings of an existing filter, click the pencil icon next to it.
	How to create a filter?
	All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.
	To create a filter:
	1. In the **Filter** drop-down list, select **Create new**.
	2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.
	3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.
	4. Select the filter creation mode: **Constructor** or **Code**.
	When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.
	5. If you selected the **Constructor** option, do the following:
	a. In the drop-down list select a boolean operator:
	• **AND**: selects events that match all of the specified conditions.
	• **OR**: selects events that match one of the specified conditions.
	• **NOT**: selects events that match none of the specified conditions.
	b. Click the **Add condition** button.
	c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.
	d. From the drop-down lists, select operands and filter operators.
	Operands of filters
	• **Event fields** specify the field of the event that you need to use as a filter operand.
	• **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl/Command+F1`**.
	If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
	• **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
	  • **dictionary** (required) is the dictionary that you want to use.
	  • **key fields** (required) are event fields that are used to generate the key of the dictionary value.
	• In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
	  • **context table name** (required) is the context table that you want to use.
	  • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
	  • **field** is the name of the context table field from which you want to get the value of the operand.
	  • **index** is the index of the list field of the table from which you want to get the value of the operand.
	• **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
	  • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
	  • **key fields** (required) are event fields that are used to generate the key of the dictionary value.
	• **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
	  • **stream** (required) is the Kaspersky CyberTrace threat category.
	  • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
	  • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press `Backspace`.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, tcp type

Destinations of the **tcp** type are used for TCP communications. Settings for a destination of the **tcp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **tcp**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**
TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values: • **Disabled** means TLS encryption is not used. This value is selected by default. • **Enabled** means TLS encryption is used, but certificates are not verified.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl`/`Command`+`F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, udp type

Destinations of the **udp** type are used for UDP communications. Settings for a destination of the **udp** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type, **udp**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl`/`Command`+`F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, http type

Destinations of the **http** type are used for HTTP communications. Settings for a destination of the **http** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **http**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.

Setting	Description
Authorization	Type of authorization when connecting to the URL specified in the **URL** field: • **Disabled**. This value is selected by default. • **Plain**. Authorization of this type is performed using the SASL/PLAIN mechanism, which transmits the user name and password in plain text. Typically, TLS is used to provide transmission security (encryption) in SASL/PLAIN. If this option is selected, in the **Secret** drop-down list, specify the secret containing user account credentials for authorization when connecting to the destination. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**

Parameter	Description

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.
	• **Custom PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format, then upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the **PFX secret** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a PFX secret?
	To create a PFX secret:
	1. In the **Name** field, enter the name of the PFX secret.
	2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key.
	3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard.
	4. Then click the **Create** button.
	The PFX secret is created and displayed in the **PFX secret** drop-down list.
	The **Custom PFX** mode is not displayed when **Authorization** is set to **Plain**.

Proxy server	The proxy server for the destination. You can select an existing proxy server or create a new proxy server. To create a new proxy server, select **Create new**. If you want to edit the settings of an existing proxy server, click the pencil icon next to it.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**

Parameter	Description
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Path	The path that must be added in the request to the URL specified in the **URL** field on the **Basic settings** tab. For example, if you specify `/input` as the path and enter `10.10.10.10` for the URL, the destination will make requests to `10.10.10.10/input`.
Health check timeout	Interval, in seconds, for checking the health of the destination.
Health check path	The URL for sending requests to obtain health information about the system that the destination resource is connecting to.
Health check	This toggle switch enables the health check. This toggle switch is turned off by default.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl/Command+F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, diode type

Destinations of the **diode** type are used to transmit events using a data diode. Settings for a destination of the **diode** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **diode**. Required setting.

Setting	Description
Data diode source directory	Path to the directory from which the data diode moves events. The maximum length of the path is 255 Unicode characters. **Limitations when using prefixes in paths on Windows servers** On Windows servers, absolute paths to directories must be specified. Directories with names matching the following regular expressions cannot be used: • `^[a-zA-Z]:\\Program Files` • `^[a-zA-Z]:\\Program Files \(x86\)` • `^[a-zA-Z]:\\Windows` • `^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` These patterns are used by the system to validate the path. The double backslashes (\\) are used as part of the regular expression syntax and must not be manually specified in the path itself. **Limitations when using prefixes in paths on Linux servers** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path.

Setting	Description
	Files are available at the following paths: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` The paths specified in the **Data diode source directory** and **Temporary directory** fields may not be the same.
Temporary directory	Path to the directory in which events are prepared for transmission to the data diode. The maximum length of the path is 255 Unicode characters. Events are stored in a file when a timeout or a buffer overflow occurs. The default timeout is 10 seconds. The prepared file with events is moved to the directory specified in the **Data diode source directory** field. The checksum (SHA-256) of the file contents is used as the name of the file with events. The paths specified in the **Data diode source directory** and **Temporary directory** fields may not be the same.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**.
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, kafka type

Destinations of the **kafka** type are used for communication using kafka. Settings for a destination of the **kafka** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **kafka**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Topic	Subject of Kafka messages. The maximum length of the subject is 255 characters. You can use the following characters: a–z, A–Z, 0–9, ".", "_", "-". Required setting.

Setting	Description
Authorization	Type of authorization when connecting to the URL specified in the **URL** field: • **Disabled**. This value is selected by default. • **Plain**. Authorization of this type is performed using the SASL/PLAIN mechanism, which transmits the user name and password in plain text. Typically, TLS is used to provide transmission security (encryption) in SASL/PLAIN. If this option is selected, in the **Secret** drop-down list, specify the secret containing user account credentials for authorization when connecting to the destination. You can select an existing secret or create a new secret. To create a new secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a secret?** *To create a secret:* 1. In the **Name** field, enter the name of the secret. 2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector. 3. If necessary, enter a description of the secret in the **Description** field. 4. Then click the **Create** button. The secret is added and displayed in the **Secret** drop-down list. • **PFX** means TLS encryption with a PFX secret. You must generate a PFX certificate with a private key in PKCS#12 container format in an external Certificate Authority, export the PFX certificate from the key store, and upload the PFX certificate to the KUMA web interface as a PFX secret. If you select this value, in the **PFX secret** drop-down list, specify a PFX secret with a certificate signed by a certification authority. You can select an existing PFX secret or create a new PFX secret. To create a new PFX secret, select **Create new**. If you want to edit the settings of an existing secret, click the pencil icon next to it. **How to create a PFX secret?** *To create a PFX secret:* 1. In the **Name** field, enter the name of the PFX secret. 2. Click **Upload PFX** and select the PKCS#12 container file to which you exported the PFX file with the private key. 3. In the **Password** field, enter the password of the PFX file that was set in the PFX Export Wizard. 4. Then click the **Create** button. The PFX secret is created and displayed in the **PFX secret** drop-down list.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**

Parameter	Description

TLS mode	TLS encryption mode. When using TLS encryption, you cannot specify an IP address in the **URL** field on the **Basic settings** tab. Available values:
	• **Disabled** means TLS encryption is not used. This value is selected by default.
	• **Enabled** means TLS encryption is used, but certificates are not verified.
	• **Custom CA** means TLS encryption is used with verification that the certificate was signed by a Certificate Authority. If you select this value, in the **Custom CA** drop-down list, specify a secret with a certificate signed by a certification authority. You can select an existing secret or create a new secret. To create a new secret, select **Create new**.
	If you want to edit the settings of an existing secret, click the pencil icon next to it.
	How to create a certificate signed by a Certificate Authority?
	You can create a CA-signed certificate on the KUMA Core server (the following command examples use OpenSSL).
	To create a certificate signed by a Certificate Authority:
	1. Generate a key to be used by the Certificate Authority, for example:
	`openssl genrsa -out ca.key 2048`
	2. Create a certificate for the generated key, for example:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< common host name of Certificate Authority >" -out ca.crt`
	3. Create a private key and a request to have it signed by the Certificate Authority, for example:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< common host name of KUMA server >" -out server.csr`
	4. Create the certificate signed by the Certificate Authority. You need to include the domain names or IP addresses of the server for which you are creating the certificate in the `subjectAltName` variable, for example:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Upload the created `server.crt` certificate in the KUMA web interface to a secret of the **certificate** type, then in the **Custom CA** drop-down list, select the secret of the **certificate** type.
	To use KUMA certificates on third-party devices, you must change the certificate file extension from CERT to CRT. Otherwise, you can get the `x509: certificate signed by unknown authority` error.

Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip** • **LZ4** • **zstd** If you do not select a value, compression is disabled (default setting).
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description

Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**.
	If you want to edit the settings of an existing filter, click the pencil icon next to it.
	How to create a filter?
	All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.
	To create a filter:
	1. In the **Filter** drop-down list, select **Create new**.
	2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.
	3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.
	4. Select the filter creation mode: **Constructor** or **Code**.
	When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.
	5. If you selected the **Constructor** option, do the following:
	a. In the drop-down list select a boolean operator:
	• **AND**: selects events that match all of the specified conditions.
	• **OR**: selects events that match one of the specified conditions.
	• **NOT**: selects events that match none of the specified conditions.
	b. Click the **Add condition** button.
	c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.
	d. From the drop-down lists, select operands and filter operators.
	Operands of filters
	• **Event fields** specify the field of the event that you need to use as a filter operand.
	• **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl/Command+F1`**.
	If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
	• **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
	  • **dictionary** (required) is the dictionary that you want to use.
	  • **key fields** (required) are event fields that are used to generate the key of the dictionary value.
	• In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
	  • **context table name** (required) is the context table that you want to use.
	  • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
	  • **field** is the name of the context table field from which you want to get the value of the operand.
	  • **index** is the index of the list field of the table from which you want to get the value of the operand.
	• **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
	  • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
	  • **key fields** (required) are event fields that are used to generate the key of the dictionary value.
	• **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
	  • **stream** (required) is the Kaspersky CyberTrace threat category.
	  • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
	  • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press `Backspace`.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, file type

Destinations of the **file** type destinations are used for writing to a file. Settings for a destination of the **file** type are described in the following tables.

> When deleting a destination of the **file** type that is being used in a service, you must restart the service.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **file**. Required setting.

Setting	Description
URL	Path to the file to which the events must be written. **Limitations when using prefixes in file paths** Prefixes that cannot be used when specifying paths to files: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` These prefixes are used by the system as regular expressions for checking the path. The * character in prefixes matches any sequence of characters and must not be manually specified in the path itself if it is not part of a valid path. Files are available at the following paths: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Output format	Format in which events are sent to the destination: • **JSON**. • **CEF**. If this value is selected, the transmitted events contain the CEF header and only non-empty fields. • **Syslog-CEF**
Delimiter	The character that marks the boundary between events: • **\n** • **\t** • **\0** If you do not select a value in this drop-down list, an empty value is selected by default. In this case, the connector does not split one event into several and passes it to the normalizer unchanged.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **`Backspace`**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, storage type

Destinations of the **storage** type are used to transfer data to storage. Settings for a destination of the **storage** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **storage**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Proxy server	The proxy server for the destination. You can select an existing proxy server or create a new proxy server. To create a new proxy server, select **Create new**. If you want to edit the settings of an existing proxy server, click the pencil icon next to it.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Health check timeout	Interval, in seconds, for checking the health of the destination.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, correlator type

Destinations of the **correlator** type are used to transfer data to a correlator. Settings for a destination of the **correlator** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **correlator**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Proxy server	The proxy server for the destination. You can select an existing proxy server or create a new proxy server. To create a new proxy server, select **Create new**. If you want to edit the settings of an existing proxy server, click the pencil icon next to it.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Health check timeout	Interval, in seconds, for checking the health of the destination.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **`Backspace`**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Destination, eventRouter type

Destinations of the **eventRouter** type are used for sending events to the event router. Settings for a destination of the **eventRouter** type are described in the following tables.

Basic settings tab

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
State	This toggle switch enables sending events to the destination. This toggle switch is turned on by default.
Type	Destination type: **eventRouter**. Required setting.
URL	URL (required)—a URL that you need to connect to. The following URL formats are supported: • `< host name >:< port number >` • `< IPv4 address >:< port number >` • `< IPv6 address >:< port number >` You can specify IPv6 addresses in the following format: `[< IPv6 address >%< interface >:< port number >`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. You can add multiple URLs and remove an URL. KUMA does not allow saving a resource or service if the URL field contains a tab or space character. To add an URL, click the **+ Add** button. To remove an URL, click the delete ✕ icon next to it. Required setting.
Tags	Tags for resource search. Optional setting.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.

Advanced settings tab

Parameter	Description
Buffer size	Buffer size in bytes for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. Default buffer size: 67,108,864 (64 MB), displayed as 0 in the interface.
Buffer flush interval	Interval (in seconds) for sending events to the destination. The default value is 1 second.
Disk buffer size limit	Size of the disk buffer in bytes. Default value: 10 GB, displayed as 0 in the interface.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. The value must be a positive integer up to 999.
Proxy server	The proxy server for the destination. You can select an existing proxy server or create a new proxy server. To create a new proxy server, select **Create new**. If you want to edit the settings of an existing proxy server, click the pencil icon next to it.
Compression	Determines whether the stream of events is sent by the KUMA agent to the destination in compressed form. Available values: • **Disabled**. • **Snappy** • **gzip**
URL selection policy	Method of determining URLs to which events must be sent first if you added multiple URLs in the **URL** field on the **Basic settings** tab: • **Any** means events are sent to a randomly selected available URL as long as the URL accepts events. If the URL becomes unavailable, events are sent to another randomly selected available URL. This value is selected by default. • **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next added available URL. If the first added URL becomes available again, events are sent to the first added URL again. • **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.
Health check timeout	Interval, in seconds, for checking the health of the destination.
Disk buffer disabled	This toggle switch that enables the disk buffer. This toggle switch is turned on by default. The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.
Timeout	The time, in seconds, for which the destination waits for a response from another service or component.
Debug	The switch enables resource logging. The toggle switch is turned off by default.

Parameter	Description
Filter	Filter for determining which events must be processed by the resource. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press `Ctrl/Command+F1`. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Parameter	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when managing the settings of a destination and is used for linking to services, that is, collectors, correlators, and event routers.

To link a destination to a service, click the **Link to service** button → **Link to <service_name>**. This opens a window; in that window, select one or more services and click **OK**. The destination is linked to the selected services.

If necessary, you can unlink the destination from a service. To do this, select the check box next to the service, click **Delete** and confirm the unlinking from the service.

Using a proxy server

Proxy servers are used to store proxy server configuration settings, for example, in destinations. The http type is supported.

To create a proxy server:

1. In the web interface, go to **Resources** → **Proxy servers**, and click the **Create** button.
2. In the **Name** field, enter a unique name for the proxy server. Maximum length of the name: 128 Unicode characters.
3. In the **Tenant** drop-down list, select the tenant that owns the proxy server.
4. Configure the settings for connecting to the proxy server as follows:
   - If you want to store the proxy server URL and credentials separately, select the **Secret separately** check box and fill in the following fields:
     a. In the **URL** field, specify the proxy server URL.
     b. In the **Secret** drop-down list, select a secret or create a new one with the **credentials** type by clicking the **Create** button.

     How to create a secret?

     To create a secret:

     1. In the **Name** field, enter the name of the secret.
     2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector.
     3. If necessary, enter a description of the secret in the **Description** field.
     4. Then click the **Create** button.

     The secret is added and displayed in the **Secret** drop-down list.

     If the **Secret separately** check box is selected, information about the connection to the proxy server is displayed in the interface, so when you change the password, you only need to update the secret without recreating the connections. This check box is cleared by default.

- If you want to store the proxy server URL as a secret, in the **Use URL from the secret** drop-down list, select the secret resource.

  You can create or edit a secret. To create a secret, click the **Create** button, and to edit the secret, click the pencil icon ( ).

  > We do not recommend using this option. Instead, manually specify the URL and the secret separately by selecting the **Secret separately** check box.

5. In the **Do not use for domains** drop-down list, select the domains on which the proxy server should not be used.

6. If necessary, enter a description of the proxy server in the **Description** field. Maximum length of the description: 4000 Unicode characters.

7. Click the **Create** button.

Using a dictionary

Dictionaries are resources storing data that can be used by other Kaspersky SIEM resources and services.

The KUMA distribution kit includes predefined dictionaries that you can also use when creating a correlation rule, a normalizer, an enrichment rule, or a filter.

Predefined dictionaries

Predefined dictionaries

Dictionary name	Type	Description
[OOTB] Ahnlab. Severity	dictionary	Contains a table of correspondence between a priority ID and its name.
[OOTB] Ahnlab. SeverityOperational	dictionary	Contains values of the SeverityOperational parameter and a corresponding description.
[OOTB] Ahnlab. VendorAction	dictionary	Contains a table of correspondence between the ID of the operation being performed and its name.
[OOTB] Cisco ISE Message Codes	dictionary	Contains Cisco ISE event codes and their corresponding names.
[OOTB] DNS. Opcodes	dictionary	Contains a table of correspondence between decimal opcodes of DNS operations and their IANA-registered descriptions.
[OOTB] IANAProtocolNumbers	dictionary	Contains the port numbers of transport protocols (TCP, UDP) and their corresponding service names, registered by IANA.
[OOTB] Juniper - JUNOS	dictionary	Contains JUNOS event IDs and their corresponding descriptions.
[OOTB] KEDR. AccountType	dictionary	Contains the ID of the user account type and its corresponding type name.
[OOTB] KEDR. FileAttributes	dictionary	Contains IDs of file attributes stored by the file system and their corresponding descriptions.
[OOTB] KEDR. FileOperationType	dictionary	Contains IDs of file operations from the KATA API and their corresponding operation names.
[OOTB] KEDR. FileType	dictionary	Contains modified file IDs from the KATA API and their corresponding file type descriptions.
[OOTB] KEDR. IntegrityLevel	dictionary	Contains the SIDs of the Microsoft Windows INTEGRITY LEVEL parameter and their corresponding descriptions.
[OOTB] KEDR. RegistryOperationType	dictionary	Contains IDs of registry operations from the KATA API and their corresponding values.
[OOTB] Linux. Sycall types	dictionary	Contains Linux call IDs and their corresponding names.

[OOTB] MariaDB Error Codes	dictionary	The dictionary contains MariaDB error codes and is used by the [OOTB] MariaDB Audit Plugin syslog normalizer to enrich events.
[OOTB] Microsoft SQL Server codes	dictionary	Contains MS SQL Server error IDs and their corresponding descriptions.
[OOTB] MS DHCP Event IDs Description	dictionary	Contains Microsoft Windows DHCP server event IDs and their corresponding descriptions.
[OOTB] S-Terra. Dictionary MSG ID to Name	dictionary	Contains IDs of S-Terra device events and their corresponding event names.
[OOTB] S-Terra. MSG_ID to Severity	dictionary	Contains IDs of S-Terra device events and their corresponding Severity values.
[OOTB] Syslog Priority To Facility and Severity	table	The table contains the **Priority** values and the corresponding **Facility and Severity** field values.
[OOTB] VipNet Coordinator Syslog Direction	dictionary	Contains direction IDs (sequences of special characters) used in ViPNet Coordinator to designate a direction, and their corresponding values.
[OOTB] Wallix EventClassId - DeviceAction	dictionary	Contains Wallix AdminBastion event IDs and their corresponding descriptions.
[OOTB] Windows.Codes (4738)	dictionary	Contains operation codes present in the MS Windows audit event with ID 4738 and their corresponding names.
[OOTB] Windows.Codes (4719)	dictionary	Contains operation codes present in the MS Windows audit event with ID 4719 and their corresponding names.
[OOTB] Windows.Codes (4663)	dictionary	Contains operation codes present in the MS Windows audit event with ID 4663 and their corresponding names.
[OOTB] Windows.Codes (4662)	dictionary	Contains operation codes present in the MS Windows audit event with ID 4662 and their corresponding names.
[OOTB] Windows. EventIDs and Event Names mapping	dictionary	Contains Windows event IDs and their corresponding event names.
[OOTB] Windows. FailureCodes (4625)	dictionary	Contains IDs from the **Failure Information\Status** and **Failure Information\Sub Status** fields of Microsoft Windows event 4625 and their corresponding descriptions.
[OOTB] Windows. ImpersonationLevels (4624)	dictionary	Contains IDs from the **Impersonation level** field of Microsoft Windows event 4624 and their corresponding descriptions.
[OOTB] Windows. KRB ResultCodes	dictionary	Contains Kerberos v5 error codes and their corresponding descriptions.
[OOTB] Windows. LogonTypes (Windows all events)	dictionary	Contains IDs of user logon types and their corresponding names.
[OOTB] Windows_Terminal Server. EventIDs and Event Names mapping	dictionary	Contains Microsoft Terminal Server event IDs and their corresponding names.
[OOTB] Windows. Validate Cred. Error Codes	dictionary	Contains IDs of user logon types and their corresponding names.
[OOTB] ViPNet Coordinator Syslog Direction	dictionary	Contains direction IDs (sequences of special characters) used in ViPNet Coordinator to designate a direction, and their corresponding values.
[OOTB] Syslog Priority To Facility and Severity	table	Contains the Priority values and the corresponding Facility and Severity field values.

To create a dictionary:

1. In the solution web interface, go to **Resources** → **Dictionaries**, and click the **Create** button.
2. Specify a unique dictionary name in the **Name** field. Maximum length of the name: 128 Unicode characters.
3. In the **Tenant** drop-down list, select the **tenant** that owns the dictionary.
4. In the **Description** field, enter a description of the dictionary. Maximum length of the description: 4000 Unicode characters.
5. Select tags for the dictionary from the **Tags** drop-down list.
6. In the **Type** drop-down list, select the dictionary type.
   - **Dictionary**

You can add **Key–Value** pairs. We do not recommend adding more than 50,000 entries to dictionaries of this type using the web interface.

> When adding lines with the same keys to the dictionary, each new line will overwrite the existing line with the same key. This means that only one line will be added to the dictionary.

- **Table**

  You can add data in the form of complex tables and work with such dictionaries through the REST API. When adding entries via API, there is no limit on their number. You can use REST API to read and modify the contents of dictionaries of the **Table** type, even when they are used by active services. This enables the use of dynamically updated tables uploaded from third-party applications for event enrichment.

7. In the **Value** settings block, configure the following settings:

- If you want to upload a prepared file with a dictionary, select the **Import CSV** option and import the file.

  The format of the CSV file depends on the dictionary type:

  For **Dictionary** type:

  ```
  {KEY},{VALUE}\n
  ```

  For **Table** type:

  ```
  {Column header 1}, {Column header N}, {Column header N+1}\n
  {Key1}, {ValueN}, {ValueN+1}\n
  {Key2}, {ValueN}, {ValueN+1}\n
  ```

  The keys must be unique both in the imported CSV file and in the dictionary. In tables, the key is specified in the first column. The key length must be between 1 and 128 Unicode characters, and the value length must be between 0 and 256 Unicode characters.

  When you import a dictionary, its data is completely overwritten with the contents of the file, and the resource name is replaced with the name of the imported file.

  If invalid lines are found in the imported file (for example, lines containing incorrect delimiters), they are skipped during import into a dictionary, while during import into a table they cause an error and stop the import process.

- If you want to add dictionary data manually, select **Enter data manually** and perform the following steps depending on the selected dictionary type:

  - For the **Dictionary** type, add **Key–Value** pairs.

    Specify a unique key and the corresponding value. If necessary, you can add multiple pairs. To add a new table row, click the **Add row** button.

    The maximum key length is 128 Unicode characters, and the value length is 255 Unicode characters. The first character of the key and of the value cannot be `$`.

    To delete a row, select the check box next to it and click **Delete**.

  - For the **Table** type, enter the table data.

    Enter table data. You can add and delete rows and columns, and change column headers.

    To add a new row or column, click **Add row** or **Add column**. To delete a row, select the check box next to it and click **Delete**. To delete a column, click the three-dot icon next to the column header and select **Delete**.

8. Click the **Create** button.

After you create a dictionary, you can export it by clicking **Export CSV** in the editing window. When exporting, key and value entries that contain a comma (,) or quotation marks (") are enclosed in double quotation marks. Internal quotation marks are escaped by doubling them (""").

Configuring detection logic and correlation rules

The *Correlator* is an application component that analyzes normalized events. As part of the correlation process, an event can be correlated with information from active lists and/or dictionaries.

The correlation analysis produces information that can be used for the following purposes:

- Generating alerts.
- Notifying about alerts.
- Managing active list content.
- Sending correlation events to configured destinations.

Events are correlated in real time. The operating principle of the correlator is based on signature analysis of events. This means that every event is processed in accordance with the correlation rules created by the user.

When a sequence of events is detected that satisfies the conditions of a correlation rule, the correlator creates a correlation event. Depending on the configuration, a correlation event can be sent to the configured destination, sent for reanalysis to the correlator, or used for further processing.

The correlation event can be sent to the correlator for reanalysis, which makes it possible to configure correlation rules to be triggered by prior analysis results. Products of one correlation rule can be used by other correlation rules.

In KUMA, you can create a standard correlator and/or a correlator NG (new generation of the correlator). The standard correlator and correlator NG use different configuration schemes and resource sets.

The correlator NG uses NG versions of resources. These resources are created and configured in KUMA and have features that make them different from the corresponding resources of the standard correlator.

> Correlator NG is not a drop-in replacement for the standard correlator. Migrating from a standard correlator to correlator NG may require checking and fixing the configuration.

Correlation rules and the resources that they use can be distributed among correlators in order to balance the load between services. Some special considerations are involved in load balancing depending on the correlator implementation.

Algorithm of correlator operation

A correlator iterates over the following steps:

1 Get an event

The correlator receives a normalized event from a collector or another service.

2 Apply correlation rules

The correlator analyzes the received event to match it against the conditions of correlation rules. Rules can be configured for analyzing individual events or sequences of events. If the conditions of the rule are satisfied, the correlator generates the correlation result and performs the actions specified by the configuration of the rule.

3 Processing the correlation result

Depending on the configuration of the rule, the correlator can:

- Enrich the event
- Perform operations with active lists
- Perform operations with context tables
- Generate a correlation event
- Pass the result to further processing

Additional actions can be performed using customized enrichment, response, and routing rules.

4 Send a correlation event

If the analysis reveals a sequence of events that satisfies the conditions of a correlation rule, the correlator creates a correlation event.

Depending on the configuration of the correlator, the correlation event can be sent to the configured destination or sent to the correlator to be analyzed again. When analyzed again, the correlation event can be used by other correlation rules.

Creating a correlator

You can create a correlator in the Kaspersky SIEM web interface in one of the following ways:

- In the **Resources** section, click **Add correlator**.
- In the **Resources** → **Correlators** section on the **Current** tab, click **Create**.

Creating a correlator involves the following steps:

1 Managing the basic correlator settings

1. On the **Basic settings** tab, in the **General** section, fill in the following fields:

   - In the **Name** field, enter a unique name for the correlator. The name must contain 1 to 128 Unicode characters.

   - In the **Tenant** drop-down list, select the tenant that must own the correlator. The tenant selection determines what resources will be available when the collector is created.

     > If, when creating a correlator, you go back to the General section and select a different tenant, you must manually update all resources that you added to the service. Only resources from the selected tenant and the Shared tenant can be added to the service.

   - If necessary, in the **Workers** field, specify the number of workers that the correlator can run simultaneously to process events in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.

   - In the **GeoIP download timeout** field, specify the timeout for geodata (GeoIP) downloading when executing enrichment rules with a **geodata** data source type. The default value is 120 seconds.

   - If necessary, select the tags for the correlator from the **Tags** drop-down list.

   - If necessary, in the **Description** field, add a description for the service up to 256 Unicode characters long.

2. On the **Advanced settings** tab, fill in the following fields:

   - If necessary, use the **Debug** toggle switch to enable logging of service operations.

   - You can use the **Create dump periodically** toggle switch at the request of Technical Support to generate resource (CPU, RAM, etc.) utilization reports in the form of dumps.

   - In the **Dump settings** field, you can specify the settings to be used when creating dumps. The specifics of filling in this field must be provided by Technical Support.

   - In the **Number of incoming requests in a queue in a queue** field, specify the maximum number of database insert queries that can be queued for processing by the correlator.

2 Adding global variables

If tracking values in event fields, active lists, or dictionaries is not enough for certain security scenarios, you can use global and local variables. Such variables allow performing different actions on the values received by the correlators, implementing complex threat detection logic. Variables can be assigned a specific function and then queried from correlation rules as if they were ordinary event fields, with the triggered function result received in response.

To add a global variable in the correlator:

1. In the **Global variables** section, click the **Add** button.

2. Specify the following settings:

   a. In the **Variable** window, enter the name of the variable.

      Variable naming requirements

      - Must be unique within the correlator.
      - Must contain 1 to 128 Unicode characters.
      - Must not begin with the character $.
      - Must be written in camelCase or CamelCase.

   b. In the **Value** window, enter the variable function.

      When entering functions, you can use autocomplete as a list of hints with possible function names, their brief description and usage examples. You can select a function from the list and insert it together with its list of arguments into the input field.

      To display the list of all hints in the field, press **`Ctrl+Space`**. Press **`Enter`** to select a function from the list. Press **`Tab`** to go to the next argument in the list of arguments of the selected function.

      Description of variable functions.

The global variable is added. It can be referenced in correlation rules by adding the $ character in front of the variable name. There can be multiple variables. Added variables can be edited or deleted by using the × icon.

3 Adding a correlation rule

You can select or create correlation rules. They define sequences of events that indicate security-related incidents. When these sequences are detected, the correlator creates a correlation event and an alert.

If you have added global variables to the correlator, all added correlation rules can reference them.

To add a correlation rule:

1. In the **Correlation** section, click the **Add** button.

2. Specify the settings for the correlation rule. The available settings depend on the selected type of correlation rule:

   - standard
   - simple
   - operational

The correlation rule will be created and linked to the resource set for the correlator. It is displayed in the correlation rules table and in the list of resources under **Resources** → **Correlation rules**.

You can use the **Search** field to search for a correlation rule. Added correlation rules can be removed from the resource set by selecting the relevant rules and clicking **Delete**.

Selecting a correlation rule opens a window with its settings, which can be edited and then saved by clicking **Save**. If you click **Delete** in this window, the correlation rule is unlinked from the resource set.

Use the **Move up** and **Move down** buttons to change the position of the selected correlation rules in the table. It affects their execution sequence when events are processed. Using the **Move operational to top** button, you can move correlation rules of the **operational** type to the beginning of the correlation rules list.

4 Event enrichment (optional step)

You can select or create enrichment rules and indicate which data from which sources you want to add to correlation events that the correlator creates. There can be more than one enrichment rule. You can add them by clicking the **Add enrichment** button and can remove them by clicking the × button.

To add an enrichment rule:

1. In the **Enrichment** section, click the **Add enrichment** button.
2. In the **Enrichment rule** drop-down list, select the required rule or create a new one by clicking **New**.

   If you select an enrichment rule from the list, the **Enrichment** section displays the settings of the selected rule.
3. In the **Name** field, enter a unique name for the enrichment rule.
4. In the **Source kind** drop-down list, select the source of data for enrichment and define its corresponding settings:

   template

   This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

   Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

   If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

   - `{{.SA.StringArrayOne}}`
   - `{{- range $index, $element := . SA.StringArrayOne -}}`
     `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

table

This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "table"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.
Mapping	Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`).

The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field.

If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

constant

This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "constant"

Setting	Description
Constant	The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed.
Target field	The event field to insert the data into.

If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field.

If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array.

dictionary

This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dictionary"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.

If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`.

If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`.

event

This type of enrichment is used when you need to write a value from another event field to the current event field. The settings of the enrichment type are described in the table below.

Parameters of enrichment type "event"

Setting	Description
Target field	The event field where the data needs to be inserted.
Source field	The event field whose value is written to the target field.
Conversion	The block of settings where you can create rules for modifying the original data before it is written to event fields. The conversion type can be selected from the drop-down list. You can use the **Add conversion** and **Delete** buttons to add or delete a conversion, respectively. The order of conversions is important.

Whether or not a conversion can be used depends on the type of an extended event schema field being used:

- For an additional field of the `String` type, all types of conversion are available.
- For the `Number` and `Float` type fields, the following types of conversion are available: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String**, and **decodeBase64URLString**.
- For the `Array of strings`, `Array of numbers`, and `Array of floats` type fields, the following types of conversion are available: **append**, and **prepend**.

View available transformations

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

- **lower**—is used to make all characters of the value lowercase

- **upper**—is used to make all characters of the value uppercase

- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.
- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

dns

This type of enrichment is used to send requests to a private network DNS server to convert IP addresses into domain names or vice versa. IP addresses are converted to DNS names only for private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dns"

Setting	Description
URL	URL of the DNS server to which you want to send requests. You can use the **Add URL** button to specify multiple URLs. If the **URL** setting is not specified, KUMA takes the list of DNS servers from the localhost's `/etc/resolv.conf` file. In this case, you need to enable the **Recursive queries** option. Otherwise, the enrichment will not occur.
Requests per second	Maximum number of queries sent to the DNS server per second. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Workers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used. The default value is `1`.
Maximum number of events in enrichment queue	The maximum number of events to hold in the resubmission queue. The default value is `1,000,000`.
Timeout	The time to wait for a response from the DNS server (in seconds). The default value is `5`.
DNS mode override	Resolution method used: • **Forward DNS only** resolves a domain name to an IP address. • **Reverse DNS only** resolves an IP address to a domain name. • **Forward and reverse DNS** resolves a domain name to an IP address or an IP address to a domain name.
Cache TTL	The lifetime (in seconds) of values stored in the cache. The default value is `60` seconds.
Cache disabled	You can enable or disable caching using this setting. Caching is enabled by default.

Setting	Description
Cache refresh disabled	If cache update is enabled, then upon expiry of the cache's TTL the collector sends repeated requests to the DNS server to update the data stored in the cache. This setting is available only when cache is enabled. By default, cache update is enabled.
Recursive queries	Allows a collector to send recursive queries to authoritative DNS servers for the purposes of enrichment. The default value is **Disabled**.

cybertrace

> For systems with high load on a collector or correlator, we recommend using the **cybertrace-http** enrichment type. This type of enrichment returns a structured JSON response and correctly distinguishes between strings and arrays of custom attributes, preventing parsing errors.
> When **cybertrace** enrichment is used, the collector receives an unstructured response. If the value of a custom attribute in Kaspersky CyberTrace contains square brackets, for example, **[str1**, **str2]**, Kaspersky SIEM treats it as an array, not a string.

This type of enrichment is used to add information from Kaspersky CyberTrace data feeds to event fields. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace"

Setting	Description
URL	URL of the Kaspersky CyberTrace server which you want to send requests to. The default Kaspersky CyberTrace port is 9999. Required setting.
Number of connections	Maximum number of connections to the Kaspersky CyberTrace server that can be established simultaneously by Kaspersky SIEM. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Requests per second	Maximum number of requests sent to the server per second. The default value is `1000`.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`.
Mapping	Table for mapping event fields to the types of indicators in Kaspersky CyberTrace. The **KUMA field** column shows the names of event fields, and the **CyberTrace indicator** column shows the types of Kaspersky CyberTrace indicators. Available types of Kaspersky CyberTrace indicators: • **ip** • **url** • **hash**

In the mapping table, you must provide at least one string. You can add new table rows or delete table rows. To add a new table row, click **Add row**. To delete a row in the table, click the ✕ cross.

cybertrace-http

This streaming event enrichment type in Kaspersky CyberTrace allows you to send a large number of events to the CyberTrace API-interface with a single request. We recommend using the **cybertrace-http** enrichment type for systems with a large stream of events. The **cybertrace-http** enrichment type performs better than the **cybertrace** enrichment type.

Limitations:

- The **cybertrace-http** enrichment type cannot be used for retrospective scanning in KUMA.
- When the **cybertrace-http** enrichment type is used, cyberthreat detections are not saved in Kaspersky CyberTrace history in the **Detections** window.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace-http"

Setting	Description
Tenant	Tenant, within which you plan to work with Kaspersky CyberTrace. Required setting.
URL	URL of the Kaspersky CyberTrace server to which you want to send requests, and the port used by the CyberTrace API. The default port is 443. Required setting.
Secret	The drop-down list where you can select the secret that stores the connection credentials. Required setting.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Key fields	The list of event fields used for enriching events with data from Kaspersky CyberTrace. Required setting.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`. After reaching 1 million events received from the Kaspersky CyberTrace server, events stop being enriched until the number of received events is reduced to less than 500,000.
CyberTrace main version	Kaspersky CyberTrace version. Available values: • **<5**—requests are executed in the General tenant in Kaspersky CyberTrace, and use the new API version provided by Kaspersky CyberTrace 5.0 and later. • **≥ 5.0**—requests use the API version that corresponds to Kaspersky CyberTrace 4.x. The default value is **<5**.
Debug	The parameter that enables resource logging. The toggle switch is turned off by default.
Tags	Tags for resource search.

timezone

This type of enrichment is used in collectors and correlators to assign a specific time zone to an event. Time zone information may be useful when searching for events that occurred at unusual times, such as nighttime.

When this type of enrichment is selected, the required time zone must be selected from the **Time zone** drop-down list.

> Make sure that the selected time zone is set on the server hosting the enrichment-utilizing service. For example, you can do this by using the `timedatectl list-timezones` command, which shows all time zones that are set on the server. For more details on setting time zones, please refer to your operating system documentation.

When an event is enriched, the time offset of the selected time zone relative to Coordinated Universal Time (UTC) is written to the DeviceTimeZone event field in the `+-hh:mm` format. For example, if you select the **Asia/Yekaterinburg** time zone, the value `+05:00` will be written to the `DeviceTimeZone` field. If an enriched event already has a value in the `DeviceTimeZone` field, it will be overwritten.

By default, if the timezone is not specified in the event being processed and enrichment rules by timezone are not configured, the event is assigned the timezone of the server hosting the service (collector or correlator) that processes the event. If server time is changed, the service must be restarted.

Permissible time formats when enriching the DeviceTimeZone field

When processing incoming raw events in the collector, the following time formats can be automatically converted to the `+-hh:mm` format (see the table below):

Time format in a processed event	Example
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

If the date format in the `DeviceTimeZone` field differs from those listed in the table, the collector server time zone is written to the field when an event is enriched with time zone information. You can create normalization rules for non-standard time formats.

geographic data

This type of enrichment is used to add IP address geographic data to event fields.

When this type is selected under **Mapping geographic data to event fields** parameter block, you need to specify from which event field the IP address will be read, select the attributes of geographic data, and define the event fields to which geographic data will be written:

1. In the **Event field with IP address** drop-down list, select the event field from which the IP address is read. Geographic data uploaded to KUMA is matched against this IP address.

   > When the `SourceAddress`, `DestinationAddress`, and `DeviceAddress` event fields are selected, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields.

2. For each event field you need to read the IP address from, select the type of geographic data and the event field to which the geographic data should be written.

   - In the **Geodata attribute** field, select which geographic data corresponding to the read IP address should be written to the event. Available geographic data attributes: **Country**, **Region**, **City**, **Longitude**, **Latitude**.
   - In the **Event field to write to**, select the event field which the selected geographic data attribute must be written to.

   You can use the **Add geodata attribute** button to add field pairs for **Geodata attribute** – **Event field to write to**. You can also configure different types of geographic data for one IP address to be written to different event fields.

3. To add each subsequent mapping, click the **Add mapping** button and repeat the previous two steps of these instructions.

   You can write identical geographic data attributes to different event fields. If you configure multiple geographic data attributes to be written to the same event field, the event will be enriched with the last mapping in the sequence.

check DLL Hijacking

DLL Hijacking is an attack technique that involves delivering vulnerable legitimate software along with a malicious dynamic link library (DLL) to a target system. To detect such attacks, Kaspersky SIEM uses the AI module. The AI module analyzes the launch and runtime parameters of applications and identifies suspicious launches of legitimate software with malicious libraries.

To get a status, Kaspersky SIEM sends a request with information from event fields to <KSN>. In response to the request, KSN sends the analysis result.

You can configure DLL Hijacking attack detection in the collector or correlator.

To use enrichment such as **check DLL Hijacking**, your license must include the AI module. The General administrator needs also to accept the additional KSN Statement in the **Kaspersky Security Network** section (**Settings** → **Integrations** → **AI services** → **DLL Hijacking detection**).

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "DLL Hijacking"

Setting	Description
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.
Maximum cache size	Maximum cache size for KSN responses, in megabytes. The default value is `128 MB`. Each KSN response has its own lifetime, during which it is retained in the cache. If Kaspersky SIEM sends a second request for a DLL file for which KSN has already issued a response, and the lifetime of that response has not yet expired, the request is not actually sent to KSN, but the response is taken from the cache.
Maximum number of events in enrichment queue	If the specified value is exceeded, new events are not processed. The default value is `1,000,000`. `0` means that event processing stops if the queue contains any number of events.

Perform a repeat request	KSN response may return the **Unclassified** status. This status means that KSN has accepted the request and is currently processing it, but there is no status yet. Processing may take a long time, so the request must be re-sent.
	If this setting is enabled, specify additional settings:
	• If the **Create duplicates** setting is enabled, KUMA creates a duplicate event and uses it for repeated requests to KSN. In this case, the main event is routed in accordance with the workflow. A duplicate event is written to the database when one of the following conditions is satisfied:
	  • A status other than **Unclassified** is received from KSN.
	  • The disk buffer configured using the **Buffer size** setting is full.
	  • The **Request count** is exceeded.
	If this setting is disabled, KUMA continues to send requests using the main event. The event is written to the database when one of the following conditions is satisfied:
	• A status other than **Unclassified** is received from KSN.
	• The disk buffer configured using the **Buffer size** setting is full.
	• The **Request count** is exceeded.
	• The **Request count** is the maximum number of requests to KSN. If a status other than **Unclassified** is not received by executing the specified number of requests, the event is written to the database with the **Unclassified** status. The default value is `10`.
	• **Poll interval** is the interval between requests, in minutes. The default value is `1 minute`. The minimum value is `1 minute`.
	• **Buffer size** is the size of the disk buffer for events awaiting a repeat request, in megabytes. The default value is `10240 MB`. The minimum value is `10 MB`.

Proxy server	Proxy server settings, if one is needed to connect to the KSN server. You can select one of the available proxy servers or create a new proxy server. By default, a proxy server is not used.

Mapping	The table of parameters that must be sent in a KSN request to get a status, and a list of the corresponding KUMA event fields. • **DLL file hash (md5)**—a recommended mapping field: `OldFileHash`. • **DLL file path**—a full path including a file name. Recommended field for mapping: `OldFilePath`. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **Process hash (md5)**—a recommended mapping field: `FileHash`. • **process path**. Full path including the file name. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **DLL file name**—a recommended mapping field: `OldFileName`. • **Process name**—a recommended mapping field: `FileName`. • **Process signature** is a field that specifies the KUMA field that transfers the `Organization` from the signature `Subject`. If these values are not available, leave the signature empty. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** column, select **process signature** from the drop-down list (optional). Recommended field for mapping: FileID. • **dll size**. Optional; recommended field for mapping: OldFileSize. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** field, select **dll size** from the drop-down list. For each parameter, specify a corresponding KUMA event field in the table.

5. Use the **Debug** toggle switch to indicate whether or not to enable logging of service operations. Logging is disabled by default.

6. Under **Filter**, you can specify conditions to identify events that will be processed using the enrichment rule. You can select an existing filter from the drop-down list or **create** a new filter.

   Creating a filter in resources

   All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

   To create a filter:

   1. In the **Filter** drop-down list, select **Create new**.

   2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

   3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

   4. Select the filter creation mode: **Constructor** or **Code**.

      When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

   5. If you selected the **Constructor** option, do the following:

      a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

b. Click the **Add condition** button.

c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

d. From the drop-down lists, select operands and filter operators.

Operands of filters

- **Event fields** specify the field of the event that you need to use as a filter operand.
- **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

  If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.
- **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the dictionary that you want to use.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
  - **context table name** (required) is the context table that you want to use.
  - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
  - **field** is the name of the context table field from which you want to get the value of the operand.
  - **index** is the index of the list field of the table from which you want to get the value of the operand.
- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.

- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.

- **inContextTable** checks for the presence of the entry in the specified context table.
- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.

e. To add a group of conditions for the filter, click the **Add group** button.

You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ×.

8. Click **Save**.

The new enrichment rule was added to the resource set for the correlator.

5 Adding a response rule (optional step)

You can select or create response rules and indicate which actions must be performed when the correlation rules are triggered. There can be multiple response rules. You can add rules by clicking the **Add response rule** button or remove rules by clicking the × button.

To add a response rule:

1. In the **Response** section, click **Add response rule**.

2. In the **Response rule** drop-down list, select the required rule or create a new one by clicking **New**.

   If you select a response rule from the list, the **Response** section displays the settings of the selected rule.

3. In the **Type** drop-down list, select the type of response rule and define its corresponding settings:

   - **Response via KSC**—response rules for automatically launching the tasks on Kaspersky Security Center assets. For example, you can configure automatic startup of a virus scan or database update.

     Tasks are automatically started when KUMA is integrated with Kaspersky Security Center. Tasks are run only on assets that were imported from Kaspersky Security Center.

     Response settings

     - **Kaspersky Security Center task** (required)—name of the Kaspersky Security Center task that you need to start. Tasks must be created beforehand, and their names must begin with "`KUMA `". For example, "`KUMA antivirus check`".

Types of Kaspersky Security Center tasks that can be started using KUMA:

- Update
- Virus scan

- **Event field** (required)—defines the event field of the asset for which the Kaspersky Security Center task should be started. Possible values:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

> To send requests to Kaspersky Security Center, you must ensure that Kaspersky Security Center is available over the UDP protocol.

- **Run script**—response rules for automatically running a script. For example, you can create a script containing commands to be executed on the KUMA server when selected events are detected.

  The script file is stored on the server where the correlator service using the response resource is installed: /opt/kaspersky/kuma/correlator/<correlator ID>/scripts.

  The `kuma` user of this server requires the permissions to run the script.

  Response settings

  - **Timeout**—the number of seconds the system will wait before running the script.
  - **Script name** (required)—the name of the script file.

    If the script Response resource is linked to the Correlator service, but the is no script file in the /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts directory, the service will not start.
  - **Script arguments**—parameters or correlation event field values that must be passed to the script.

    > If the script includes actions taken on files, you should specify the absolute path to these files.

    Parameters can be written with quotation marks (").

    Correlation event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field which value must be passed to the script.

    Example: `-n "\"usr\": {{.SourceUserName}}"`

- **Response via KEDR**—response rules for automatically creating prevention rules, starting network isolation, or starting the application on Kaspersky Endpoint Detection and Response and Kaspersky Security Center assets.

  Automatic response actions are carried out when KUMA is integrated with Kaspersky Endpoint Detection and Response.

Response settings

- **Event field** (required)—event field containing the asset for which the response actions are needed. Possible values:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID
- **Task type**—response action to be performed when data matching the filter is received. The following types of response actions are available:
  - Enable network isolation.

    When selecting this type of response, you need to define values for the following settings:

    - **Isolation timeout**—the number of hours during which the network isolation of an asset will be active. You can indicate from 1 to 9,999 hours.

      If necessary, you can **add an exclusion for network isolation**.

      To add an exclusion for network isolation:

      a. Click the **Add exclusion** button.

      b. Select the direction of network traffic that must not be blocked:

      - Inbound.
      - Outbound.
      - Inbound/Outbound.

      c. In the **Asset IP** field, enter the IP address of the asset whose network traffic must not be blocked.

      d. If you selected **Inbound** or **Outbound**, specify the connection ports in the **Remote ports** and **Local ports** fields.

      e. If you want to add more than one exclusion, click **Add exclusion** and repeat the steps to fill in the **Traffic direction**, **Asset IP**, **Remote ports** and **Local ports** fields.

      f. If you want to delete an exclusion, click the **Delete** button under the relevant exclusion.

      > When adding exclusions to a network isolation rule, Kaspersky Endpoint Detection and Response may incorrectly display the port values in the rule details. This does not affect application performance. For more details on viewing a network isolation rule, please refer to the *Kaspersky Anti Targeted Attack Platform Help Guide*.

  - Disable network isolation.
  - Add prevention rule.

When selecting this type of response, you need to define values for the following settings:

- **Event fields to extract hash from**—event fields from which KUMA extracts SHA256 or MD5 hashes of the files that must be prevented from starting.

  The selected event fields and the values selected in the **Event field** must be added to the inherited fields of the correlation rule.

- **File hash #1**—SHA256 or MD5 hash of the file to be blocked.

At least one of the above fields must be completed.

- Delete prevention rule.

- Run program.

  When selecting this type of response, you need to define values for the following settings:

  - **File path**—path to the file of the process that you want to start.

  - **Command line parameters**—parameters with which you want to start the file.

  - **Working directory**—directory in which the file is located at the time of startup.

  When a response rule is triggered for users with the General Administrator role, the **Run program** task will be displayed in the **Task manager** section of the application web interface. In the **Created by** column of the task table, **Scheduled task** is displayed for this task . You can view task completion results.

  All of the listed operations can be performed on assets that have Kaspersky Endpoint Agent for Windows. On assets that have Kaspersky Endpoint Agent for Linux, the application can only be started.

  At the software level, the capability to create prevention rules and network isolation rules for assets with Kaspersky Endpoint Agent for Linux is unlimited. KUMA and Kaspersky Endpoint Detection and Response do not provide any notifications about unsuccessful application of these rules.

- **Response via KICS/KATA**—response rules for automatically starting tasks on KICS for Networks assets. For example, you can change the asset status in KICS for Networks.

  Tasks are automatically started when KUMA is integrated with KICS for Networks.

Response settings

- **Event field** (required)—event field containing the asset for which the response actions are needed. Possible values:
  - **SourceAssetID**
  - **DestinationAssetID**
  - **DeviceAssetID**
- **Status of the asset in KICS/KATA** is the status to be set for the specified asset. The following values are available:
  - **Unauthorized**
  - **Authorized**

  When a response rule is triggered, KUMA will send KICS/KATA an API request to change the status of the specified asset to the selected status.

- **Response via Active Directory**—response rules for changing the permissions of Active Directory users. For example, block a user.

  Tasks are started if integration with Active Directory is configured.

  Response settings

  - **Account ID source** is the event field from which the value of the Active Directory account ID is taken. Possible values:
    - **SourceAccountID**
    - **DestinationAccountID**
  - **AD command**—command that is applied to the account when the response rule is triggered. Available values
    - **Add account to group**
    - **Remove account from group**
    - **Reset account password**
    - **Block account**

4. In the **Workers** field, specify the number of workers that the correlator can run simultaneously to process events in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.

   This field is optional.

5. Under **Filter**, you can specify conditions to identify events that will be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter.

   Creating a filter in resources

All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

To create a filter:

1. In the **Filter** drop-down list, select **Create new**.

2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

4. Select the filter creation mode: **Constructor** or **Code**.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

5. If you selected the **Constructor** option, do the following:

   a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

   b. Click the **Add condition** button.

   c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

   d. From the drop-down lists, select operands and filter operators.

      Operands of filters

      - **Event fields** specify the field of the event that you need to use as a filter operand.

      - **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

        If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.

      - **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:

        - **dictionary** (required) is the dictionary that you want to use.

        - **key fields** (required) are event fields that are used to generate the key of the dictionary value.

- In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:
  - **context table name** (required) is the context table that you want to use.
  - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.
  - **field** is the name of the context table field from which you want to get the value of the operand.
  - **index** is the index of the list field of the table from which you want to get the value of the operand.
- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.

- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.

- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

  If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.

- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.

- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.

- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.

- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.

- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.

- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.

- **inContextTable** checks for the presence of the entry in the specified context table.

- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **`Backspace`**.

e. To add a group of conditions for the filter, click the **Add group** button.

   You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⣿. To remove a condition, click the delete icon ✕.

8. Click **Save**.

The new response rule was added to the resource set for the correlator.

6 Add destination (optional step)

You can select or create destinations with settings indicating the forwarding destination for events created by the correlator. Events from a correlator are usually redirected to a storage so that they can be saved and viewed later if necessary. Events can be sent to other locations as needed. There can be more than one destination point.

To add a destination:

1. In the **Routing** section, click the **Add** button.

2. In the opened window, in the **Destination** field, select the destination type that you want to add, or create a new one by clicking **Create new** and configuring the following settings:

   a. On the **Basic settings** tab, in the **Name** field, enter a unique name for the destination. The name must contain 1 to 128 Unicode characters.

   b. You can use the **State** toggle switch to enable or disable the service as needed.

   c. In the **Type** drop-down list, select the type of the destination. The following values are available:

      - internal
      - nats-jetstream
      - tcp
      - udp
      - http
      - diode
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. On the **Advanced settings** tab, specify the values of parameters. The set of parameters that can be configured depends on the type of the destination selected on the **Basic settings** tab. For detailed information about parameters and their values, click the link for each type of destination in paragraph "c." of these instructions.

The new destination is added to the resource set for the correlator.

7 Testing correlator settings

At this stage, KUMA creates a service resource set with the services being created automatically based on this set:

- The resource set for the correlator is displayed under **Resources** → **Correlators**. It can be used to create new correlator services. When this set of resources changes, all services that operate based on it will start using the new parameters after the services restart. To do so, you can use the **Save and restart services** and **Save and update service configurations** buttons.

  A resource set can be modified, copied, moved from one folder to another, deleted, imported, and exported, like other resources.

- Services are displayed in **Resources** → **Active services**. The services created using the Installation Wizard perform functions inside the KUMA solution. To communicate with external parts of the network infrastructure, you need to install similar external services on the servers and assets intended for them. For example, an external correlator service should be installed on a server intended to process events, external storage services should be installed on servers with a deployed ClickHouse service, and external agent services should be installed on Windows assets that must both receive and forward Windows events.

To test correlator settings:

1. Click **Create and save service**.

   The **Setup validation** section displays a table of services created based on the set of resources selected in the Installation Wizard. The lower part of the window shows examples of commands that you must use to install external equivalents of these services on their intended servers and assets.

   Example

   ```
   sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <CA_certificate_ID> --
   id <service_ID> --api.port <API_port> --install
   ```

   where:

   `<FQDN>` is the fully qualified domain name of the KUMA Core server.

   `<port>` is the port that KUMA Core uses for internal communications (port 7210 is used by default).

   `<CA_certificate_ID>` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

   `<service_ID>` is the service ID copied from the KUMA web interface.

   `<API_port>` is the port used for communication with the component being installed.

   > The "kuma" file can be found inside the installer in the /kuma-ansible-installer/roles/kuma/files/ directory.

   The port for communication with the KUMA Core, the service ID, the ID of the CA certificate, and the port for communication with the service are added to the command automatically. You should also ensure the network connectivity of the KUMA system and open the ports used by its components if necessary.

2. Close the correlator creation window by clicking **Create**.

After finishing creating and configuring the correlator, you need to install the KUMA correlator on the server using the command copied from the **Setup validation** section.

Creating a correlator NG

Correlator NG is the new version of the correlator for processing and correlating events.

> The version of correlator NG that ships with Kaspersky SIEM 4.6 is a beta version, which means that functionality, settings and behavior may change in future versions.

You can create a correlator NG in one of the following ways:

- In the **Resources** → **Correlators** → **NG** section, click the **Create** button to create a correlator NG from scratch.
- In the **Resources** → **Correlators** → **Current** section, select the a standard correlator that you have created and click the **Convert to NG** button.

  This opens the form for creating a correlator NG with settings migrated from the standard correlator. The original standard correlator is not modified and remains on the **Current** tab. After saving, the correlator NG appears on the **NG** tab.

Creating a correlator NG from scratch involves the following steps:

1 Managing the basic correlator settings

1. Open the **General** section.
2. In the **Name** field, enter a unique name for the correlator. The name must contain 1 to 128 Unicode characters.
3. In the **Tenant** drop-down list, select the tenant that must own the correlator. The tenant selection determines what resources will be available when the collector is created.

   > If, when creating a correlator, you go back to the **General** section and select a different tenant, you must manually update all resources that you added to the service. Only resources from the selected tenant and the Shared tenant can be added to the service.

4. If necessary, in the **Incoming request queue** field, specify the maximum number of database insert queries that can be queued for processing by the correlator.
5. If necessary, select the tags for the correlator from the **Tags** drop-down list.
6. If necessary, in the **Description** field, add a description for the service up to 256 Unicode characters long.

2 Adding a correlation rule

You can create correlation rules. They define sequences of events that indicate security-related incidents. When these sequences are detected, the correlator creates a correlation event and an alert.

To add a correlation rule:

1. In the **Correlation** section, click the **Add** button.
2. In the **Name** field, enter a unique name for the correlator. The name must contain 1 to 128 Unicode characters.
3. In the **Tenant** drop-down list, select the tenant that you want to own the correlation rule.
4. If necessary, in the **Tags** drop-down list, select the tags for the correlation rule.
5. If necessary, add a description for the correlation rule in the **Description** field.
6. Specify the settings for the correlation rule. The available settings depend on the selected type of correlation rule:

   Standard

   Correlation rules of the **Standard** type are used for identifying complex patterns in processed events.

   The search for patterns is conducted by using buckets

   Bucket is a data container that is used by the Correlation rule resources to determine if the correlation event should be created. It has the following functions:

   - Group together events that were matched by the filters in the **Selectors** group of settings of the Correlation rule resource. Events are grouped by the fields that were selected by user in the **Identical fields** field.
   - Determine the instance when the Correlation rule should trigger, affecting the events that are grouped in the bucket.
   - Perform the actions that are selected in the **Actions** group of settings.
   - Create correlation events.

   Available states of the Bucket:

   - `Empty`—the bucket has no events. This can happen only when it was created by the correlation rule triggering.
   - `Partial Match`—the bucket has some of the expected events (recovery events are not counted).
   - `Full Match`—the bucket has all of the expected events (recovery events are not counted). When this condition is achieved:
     - The Correlation rule triggers
     - Events are cleared from the bucket
     - The trigger counter of the bucket is updated
     - The state of the bucket becomes `Empty`

- `False Match`—this state of the Bucket is possible:
  - when the `Full Match` state was achieved but the join-filter returned false.
  - when **Recovery** check box was selected and the recovery events were received.

  When this condition is achieved the Correlation rule does not trigger. Events are cleared from the bucket, the trigger counter is updated, and the state of the bucket becomes `Empty`.

*To configure a correlation rule of the **Standard** type:*

1. On the **General** tab, in the **Window (sec)** field, specify the lifetime of the bucket in seconds. The time starts counting when the bucket is created, when the bucket receives the first event.

   When the bucket lifetime expires, the trigger configured on the **Actions** → **On timeout** tab is triggered, and the bucket is deleted. Triggers configured on the **Actions** → **On every threshold** and **On subsequent thresholds** tabs can trigger more than once during the lifetime of the bucket.

2. In the **Base events keep policy** drop-down list, select which base events you want to put in the correlation event. Available values:
   - **First** puts the first base event of the event collection that triggered the creation of the correlation event into the correlation event. This value is selected by default.
   - **Last** puts the last base event of the event collection that triggered the creation of the correlation event into the correlation event.
   - **All** puts all base events of the event collection that triggered the creation of the correlation event into the correlation event.

3. In the **Order by** drop-down list, select the event field by which you want correlation rule selectors to track the changes of the situation.

   This can be useful, for example, if you want to configure a correlation rule to be triggered when several types of events occur in a sequence.

4. If you want events to arrive in the correlator in the order specified in the selectors, enable the **Expect events in the order defined in the selector** toggle switch. The toggle switch is turned off by default.

5. In the **Priority** drop-down list, select the priority that will be assigned to the correlation event:
   - **Low**
   - **Medium**
   - **High**
   - **Critical**

6. In the **Rate limit** field, set the maximum number of times per second the correlation rule can trigger.

7. If you want the rule to be triggered whenever any selector reaches the threshold, enable the **Any match** toggle switch. The toggle switch is turned off by default.

   When this toggle switch is enabled, the rule is triggered as soon as any selector reaches the specified threshold. The rule does not wait for other selectors to reach thresholds.

8. If you want to additionally check the relatedness of events received by different selectors, enable the **JOIN selector** toggle switch. The toggle switch is turned off by default.

   When this toggle switch is enabled, the **JOIN selector** group of settings is displayed, in which you can specify the condition for comparing event fields of different selectors. You can set this condition manually on the **Code** tab or build it using the graphical builder on the **Builder** tab. You can compare the values of event fields of different selectors and combine conditions with the `AND`, `OR`, and `NOT` logical operators.

   For example, you can specify a condition whereby the `srcIP` of an event from one selector must match the `dstIP` of an event from another selector.

9. Under **Identical fields**, click the **Add field** button and specify the fields by which you want base events to be combined in the same bucket.

   a. In the **Base event expression** field, enter an expression whose value will be used to group events. You can specify the base event field name, a function or operation on the fields, or a constant.

   b. In the **Correlated event field** drop-down list, select the field to which the result value will be written.

   All events with the same expression result are combined in the same bucket. The result is also written to the selected field of the correlation event. For example, if in the **Base event expression** and **Correlated event field** fields, you specify `DeviceAssetID`, events with the same `DeviceAssetID` are combined in the same bucket, and the `DeviceAssetID` value is saved in the correlation event.

   If necessary, you can add and configure multiple identical fields by clicking the **Add field** button. You can delete fields by clicking the **Delete field** button.

10. In the **Unique fields** section, click the Add field button and specify the fields that determine which events in the bucket are to be considered unique.

    a. In the **Base event expression** field, enter an expression whose value will be used to judge the uniqueness of an event.

    b. In the **Correlated event field** drop-down list, select the field to which the result value will be written.

    If the bucket already contains an event with the same value in the selected correlation event field, the new event is considered non-unique and is not added to the bucket.

    If necessary, you can add and configure multiple unique fields by clicking the **Add field** button. You can delete fields by clicking the **Delete field** button.

11. Select the **Selectors** tab and click the **Add selector** button.

    a. On the **Settings** tab, configure the conditions that must be satisfied for the selector to be triggered:

       - In the **Tag** field, specify the tag for the selector.

       - Under **Expression**, specify the event selection condition. You can enter this condition manually on the **Code** tab or build it using the graphical builder on the **Builder** tab.

         When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

       - In the **Selector threshold (event count)** field, specify the number of events that must be received for the selector to trigger. The default value is `1`.

       - If necessary, enable the **Recovery** toggle switch. The toggle switch is turned off by default.

         When the **Recovery** toggle switch is enabled, if the specified number of events is received by the selector, the bucket is reset and a correlation event is not created.

b. On the **Local variables** tab, you can add variables that will be valid inside the correlation rule.

   To add a variable, click the **+ Add variable** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete variable** button.

You can add multiple selectors by clicking the **+ Add selector** button. To reorder selectors, use the reorder icons. To remove a selector, click the delete icon next to it.

12. Select the **Actions** tab.

13. If necessary, configure triggers on the following tabs:

    - **On the first threshold** triggers when the Bucket registers the first triggering of the selector during the lifetime of the Bucket.

    - **On subsequent thresholds** triggers when the Bucket registers the second and all subsequent triggering of the selector during the lifetime of the Bucket.

    - **On every threshold** triggers every time the Bucket registers the triggering of the selector.

    - **On timeout** triggers when the lifetime of the bucket ends, and is used together with a selector that has the **Recovery** toggle switch enabled in its settings. Thus, this trigger activates if the situation detected by the correlation rule is not resolved within the specified lifetime.

14. If you want correlation events to be sent for post-processing (to external enrichment outside the correlation rule, for response purposes, and to destinations), select the **Output** toggle switch. This toggle switch is turned off by default.

15. If you want to the created correlation event to be processed by the rule chain of the current correlator, enable the **Correlate** toggle switch. This makes hierarchical correlation possible. The toggle switch is turned off by default.

    If the **Output** and **Correlate** toggle switches are selected, the correlation rule is sent to post-processing first, and then to the selectors of the current correlation rule.

16. If you want to disable the creation of alerts when the correlation rule is triggered, enable the **Suppress alert** toggle switch. This toggle switch is turned off by default.

    If you do not want to create an alert when the correlation rule is triggered, but you still want to send a correlation event to the storage, enable the **Output** and **Suppress alert** toggle switches. If you enable just the Ignore alert toggle switch, a correlation event is not saved in the storage.

17. Under **Enrichment**, click the **Add enrichment** button and follow these steps:

    a. In the **Type** drop-down list, select one of the following values:

    - For the **Expression** enrichment type, manage the following settings:

      - In the **Expression** field, enter the expression to be applied to the value. The expression can contain functions and variables.

      - In the **Target field** drop-down list, select the normalized event field to which you want the result of the expression to be written.

- For the **Template** type, manage the following settings:

  - In the **Template** field, enter field names are in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.

  - In the **Target field** drop-down list, select the event field to which you want to write the data.

  You can create multiple enrichment rules, reorder enrichment rules, or delete enrichment rules. To reorder enrichment rules, use the reorder icons. To delete an enrichment rule, click the delete icon next to it.

18. Under **Active lists update** click the + **Add active list action** button and manage the following settings:

    a. In the **Active list** drop-down list, select the required NG active list.

    b. In the **Key fields** field, specify event fields to be used to create an active list entry. The specified event fields are also used as the key of the active list entry.

    The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.

    You can add multiple key fields by clicking the **Add active list action** button. To remove a key field, click the delete icon next to it.

    c. In the **Operation** drop-down list, select the operation to be applied to the active list:

    - **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.

    - **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.

    - **Delete**—delete the Active list entry.

    d. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum** or **Set**. To create a mapping rule, click the **Add mapping** button.

    Available mapping rule settings:

    - **Field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.

    - **Expression** is the event field to which the active list field is mapped.

    You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

    You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder icons. To delete an operation with an active list, click the delete icon next to it.

19. Under **Context tables update**, click the **Add context table action** button and manage the following settings:

    a. In the **Context table** drop-down list, select an NG context table.

    b. In the **Operation** drop-down list, select the operation to be applied to the active list:

    - **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table.
    - **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
    - **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
    - **Delete**—delete the context table entry.

    c. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum, Set, or Merge**. To create a mapping rule, click the **Add mapping** button.

    Available mapping rule settings:

    - **Field** is the context table field that is mapped to an event field. The field must not contain special characters or numbers only.
    - **Expression** is the event field to which the context table field is mapped.

    You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

20. If necessary, select the **Advanced settings** tab and configure the internal workings of the correlator NG. For each setting, specify a value in accordance with the performance and high availability requirements of the correlator:

    a. In the **Tick interval (ms)** field, specify the period of the correlator's internal loop in milliseconds. The lower the value, the faster the correlator reacts to changes, but the higher the load on the CPU.

    b. In the **Heartbeat tick** field, specify the number of intervals between heartbeat messages sent by the leader node to other nodes in the Raft cluster.

    c. In the **Election tick** field, specify the number of intervals after which the node starts the election of a new leader if no heartbeat messages have been received from the leader node.

    d. In the **Proposal tick** field, specify the period for generating Raft write operations from accumulated requests. The higher the value, the more requests can be combined into one operation, but the higher the latency of their processing.

    e. In the **Bytes before proposal** field, specify the maximum amount of data that can be accumulated before generating the Raft write operation. When the specified threshold is reached, the operation is generated regardless of the configured proposal processing period.

    f. In the **Maximum size of committed entries per tick** field, specify the maximum number of writes that can be applied within one internal cycle of the correlator. Limiting this allows reducing the peak load when there are many events.

g. In the **Entries before snapshot** field, specify the number of confirmed writes after which a snapshot of the Raft log is created. The snapshot reduces the size of the log and speeds up the recovery of state.

h. In the **Shards** field, specify the number of independent parts of the correlator, each of which has its own Raft log and a set of containers. Having more shards helps spread the load, but increases resource consumption.

i. In the **Request timeout (sec)** field, enter the maximum time to wait for a response from the remote service. If a response is not received within the specified time, the request is considered to have failed.

j. In the **Snapshot request timeout (sec)** field, specify the maximum time to wait for a Raft snapshot operation to finish.

k. In the **Send queue limit** field, specify the maximum number of entries that can be queued before being sent to the destination. This limitation allows keeping memory usage manageable under high load.

21. Then click the **Create** button.

Simple

Correlation rules of the **Simple** type are used to define simple sequences of events.

*To configure a correlation rule of the **Simple** type:*

1. On the **General** tab, in the **Priority** drop-down list, select the priority that will be assigned to the correlation event:

   - **Low**
   - **Medium**
   - **High**
   - **Critical**

2. In the **Rate limit** field, set the maximum number of times per second the correlation rule can trigger.

3. Select the **Selectors** tab and manage the following settings:

   a. On the **Settings** tab, specify the conditions for identifying events to be processed using the correlation rule. You can enter this condition manually on the **Code** tab or build it on the **Builder** tab.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

   b. On the **Local variables** tab, you can add variables that will be valid inside the correlation rule.

   To add a variable, click the **+ Add** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete variable** button.

4. Select the **Actions** tab.

5. If you want correlation events to be sent for post-processing (to external enrichment outside the correlation rule, for response purposes, and to destinations), select the **Output data** toggle switch. This toggle switch is turned off by default.

6. If you want to the created correlation event to be processed by the rule chain of the current correlator, enable the **Correlate** toggle switch. This makes hierarchical correlation possible. The toggle switch is turned off by default.

   If the **Output data** and **Correlate** check boxes are selected, the correlation rule is sent to post-processing first, and then to the selectors of the current correlation rule.

7. If you want to disable the creation of alerts when the correlation rule is triggered, enable the **Ignore alert** toggle switch. This toggle switch is turned off by default.

   If you do not want to create an alert when the correlation rule is triggered, but you still want to send a correlation event to the storage, enable the **Output data** and **Ignore alert** check toggle switches. If you enable just the Ignore alert toggle switch, a correlation event is not saved in the storage.

8. Under **Enrichment**, click the **Add enrichment** button and do the following:

   a. In the **Type** drop-down list, select one of the following values:

      - For the **Expression** enrichment type, manage the following settings:

        - In the **Expression** field, enter the expression to be applied to the value. The expression can contain functions and variables.

        - In the **Target field** drop-down list, select the normalized event field to which you want the result of the expression to be written.

      - For the **Template** type, manage the following settings:

        - In the **Template** field, enter field names are in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.

        - In the **Target field** drop-down list, select the event field to which you want to write the data.

   You can create multiple enrichment rules, reorder enrichment rules, or delete enrichment rules. To reorder enrichment rules, use the reorder ⣿ icons. To delete an enrichment rule, click the delete ✕ icon next to it.

9. Under **Active lists update**, click the **+ Add active list action** button and manage the following settings:

   a. In the **Active list** drop-down list, select the required NG active list.

   b. In the **Key fields** field, specify event fields to be used to create an active list entry. The specified event fields are also used as the key of the active list entry.

      The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.

      You can add multiple key fields by clicking the **+ Add active list action** button. To remove a key field, click the delete 🗑 icon next to it.

c. In the **Operation** drop-down list, select the operation to be applied to the active list:

- **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.
- **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.
- **Delete**—delete the Active list entry.

d. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum** or **Set**. To create a mapping rule, click the **+ Add mapping** button.

Available mapping rule settings:

- **Field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.
- **Expression** is the event field to which the active list field is mapped.

You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder icons. To delete an operation with an active list, click the delete icon next to it.

10. Under **Context tables update**, click the **+ Add context table action** button and manage the following settings:

a. In the **Context table** drop-down list, select an NG context table.

b. In the **Operation** drop-down list, select the operation to be applied to the active list:

- **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table.
- **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
- **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
- **Delete**—delete the context table entry.

c. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum, Set, or Merge**. To create a mapping rule, click the **+ Add mapping** button.

Available mapping rule settings:

- **Field** is the context table field that is mapped to an event field. The field must not contain special characters or numbers only.
- **Expression** is the event field to which the context table field is mapped.

You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

11. Then click the **Create** button.

Operational

Correlation rules of the **Operational** type are used for working with active lists.

*To configure a correlation rule of the **Operational** type:*

1. Select the **Selectors** tab and manage the following settings:

   a. On the **Settings** tab, specify the conditions for identifying events to be processed using the correlation rule. You can enter this condition manually on the **Code** tab or build it on the **Builder** tab.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

   b. On the **Local variables** tab, you can add variables that will be valid inside the correlation rule.

   To add a variable, click the **+ Add** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete variable** button.

2. Select the **Actions** tab.

3. Under **Active lists update**, click the **+ Add active list action** button and manage the following settings:

   a. In the **Active list** drop-down list, select the required NG active list.

   b. In the **Key fields** field, specify event fields to be used to create an active list entry. The specified event fields are also used as the key of the active list entry.

   The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.

   You can add multiple key fields by clicking the **+ Add active list action** button. To remove a key field, click the delete 🗑 icon next to it.

   c. In the **Operation** drop-down list, select the operation to be applied to the active list:

   - **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.

   - **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.

   - **Delete**—delete the Active list entry.

   d. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum** or **Set**. To create a mapping rule, click the **+ Add mapping** button.

   Available mapping rule settings:

   - **Field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.

   - **Expression** is the event field to which the active list field is mapped.

You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder icons. To delete an operation with an active list, click the delete icon next to it.

4. Under **Context tables update**, click the **+ Add context table action** button and manage the following settings:

   a. In the **Context table** drop-down list, select an NG context table.

   b. In the **Operation** drop-down list, select the operation to be applied to the active list:

      - **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table.
      - **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
      - **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
      - **Delete**—delete the context table entry.

   c. Under **Mapping**, you can use mapping rules if in the **Operation** drop-down list, you selected **Sum, Set, or Merge**. To create a mapping rule, click the **+ Add mapping** button.

      Available mapping rule settings:

      - **Field** is the context table field that is mapped to an event field. The field must not contain special characters or numbers only.
      - **Expression** is the event field to which the context table field is mapped.

      You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete mapping**.

5. Then click the **Create** button.

7. Then click the **Create** button.

The correlation rule will be created and linked to the resource set for the correlator. It is displayed in the correlation rules table and in the list of resources under **Resources** → **Correlation rules**.

You can use the **Search** field to search for a correlation rule. Added correlation rules can be removed from the resource set by selecting the relevant rules and clicking **Delete**.

Selecting a correlation rule opens a window with its settings, which can be edited and then saved by clicking **Save**. If you click **Delete** in this window, the correlation rule is unlinked from the resource set.

Use the **Move up** and **Move down** buttons to change the position of the selected correlation rules in the table. It affects their execution sequence when events are processed. Using the **Move operational to top** button, you can move correlation rules of the **operational** type to the beginning of the correlation rules list.

3 Event enrichment

You can create enrichment rules and indicate which data from which sources you want to add to correlation events that the correlator creates. There can be more than one enrichment rule. You can add them by clicking the **Add** button and can remove them by clicking the **Delete** button.

To add an enrichment rule:

1. In the **Enrichment** section, click the **Add** button.
2. In the **Name** field, enter a unique name for the enrichment rule. The name must contain 1 to 128 Unicode characters.
3. In the **Tenant** drop-down list, select the tenant that you want to own the enrichment rule.
4. In the **Rule type** drop-down list, select the source of data for enrichment and manage its settings:

   Expression

   This enrichment method transforms the event field value using expressions and functions. The evaluation result of the expression is written to the specified event field and can be used for further processing and correlation of events.

   Settings of the "Expression" enrichment type

Setting	Description
Expression	The expression applied to convert the value. The expression can contain functions and variables.
Event field to write to	Field of the normalized event to which the evaluation result of the expression is written.

   In an expression, you can use the value of the current field using the `{value}` variable and refer to other fields of the event. Enrichment functions can be used to transform values.

   For example, to make a composite value from a host name and a domain, you can use the following expression:

   ```
   concat({SourceHostName}, ".", {SourceDomain})
   ```

   The result is written to the field specified in the **Event field to write to** setting.

   Template

   This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

   Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Event field to write to	The event field to insert the data into.

If you are using enrichment of events that have **Rule type** set to **template**, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

DNS

This type of enrichment is used to send requests to a private network DNS server to convert IP addresses into domain names or vice versa. IP addresses are converted to DNS names only for private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dns"

Setting	Description
DNS servers	URL of the DNS server to which you want to send requests. You can click the **Add DNS server** button to specify multiple URLs. If the **DNS servers** setting is not specified, KUMA takes the list of DNS servers from the localhost's `/etc/resolv.conf` file. In this case, you need to enable the **Recursive query** check box. Otherwise, the enrichment will not occur.
DNS packet limit (RPS)	The maximum number of DNS packets per second for the rule, including retries and failover.
DNS concurrency	The maximum number of event packets and individual DNS queries processed at the same time.
DNS query timeout (seconds)	The time to wait for a response from the DNS server (in seconds). The default value is `5`.
Attempts per DNS Server	The number of attempts to query each DNS server for a name, including the first attempt.
Search domains	Search domains added to relative DNS names. You can click the **Add search domain** button to specify multiple domains.
DNS mode	Resolution method used: • **Forward DNS only** resolves a domain name to an IP address. • **Reverse DNS only** resolves an IP address to a domain name. • **Forward and reverse DNS** resolves a domain name to an IP address or an IP address to a domain name.
Recursive query	This toggle switch allows the collector to send recursive queries to authoritative DNS servers for the purposes of enrichment. This toggle switch is disabled by default.
Disable cache	This toggle switch enables or disables caching. Caching is disabled by default.
Cache TTL (seconds)	The lifetime (in seconds) of values stored in the cache. The default value is `60` seconds.
Ingress queue (event packets)	The maximum number of event packets waiting for DNS processing. The minimum value is `1`.

cybertrace

This type of enrichment is used to add information from Kaspersky CyberTrace data feeds to event fields. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace"

Setting	Description
Secret	The drop-down list where you can select the secret that stores the connection credentials. Required setting.
URL	URL of the Kaspersky CyberTrace server which you want to send requests to. Required setting.
Value expressions	Expressions that are sent to CyberTrace for reputation checking. You can add multiple expressions using the **Add value expression** button.
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.
Timeout (seconds)	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
CyberTrace main version	Kaspersky CyberTrace version. Available values: • **<5** means that requests use the API version that corresponds to Kaspersky CyberTrace 4.x. • **≥ 5.0** means that requests are executed in the General tenant in Kaspersky CyberTrace, and use the new API version provided by Kaspersky CyberTrace 5.0 and later. The default value is **<5**.
Ingress bandwidth	The maximum rate of events arriving for processing by the enrichment rule.
Max buffer size (bytes)	The maximum size of the buffer for accumulating events before processing or sending them on.
Reset interval (ms)	The interval in milliseconds after which events accumulated in the buffer are passed to for further processing.
Maximum number of events for re-enrichment	Maximum number of events that are stored in the enrichment queue.
Retry interval, sec	The interval in seconds between repeat attempts to send a request to the CyberTrace server if a request fails.
Maximum number of attempts	Maximum number of connections to the Kaspersky CyberTrace server that can be established simultaneously by Kaspersky SIEM. By default, this value is equal to the number of vCPUs of the KUMA Core server.

Geographic data

This type of enrichment is used to add IP address geographic data to event fields.

When this type is selected under **Mapping geographic data to event fields** parameter block, you need to specify from which event field the IP address will be read, select the attributes of geographic data, and define the event fields to which geographic data will be written:

1. In the **Event field with IP address** drop-down list, select the event field from which the IP address is read. Geographic data uploaded to KUMA is matched against this IP address.

> When the `SourceAddress`, `DestinationAddress`, and `DeviceAddress` event fields are selected, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields.

2. For each event field you need to read the IP address from, select the type of geographic data and the event field to which the geographic data should be written.

   - In the **Geodata attribute** field, select which geographic data corresponding to the read IP address should be written to the event. Available geographic data attributes: **Country**, **Region**, **City**, **Longitude**, **Latitude**.

   - In the **Event field to write to**, select the event field which the selected geographic data attribute must be written to.

   You can use the **Add geodata attribute** button to add field pairs for **Geodata attribute** – **Event field to write to**. You can also configure different types of geographic data for one IP address to be written to different event fields.

3. To add each subsequent mapping, click the **Add mapping** button and repeat the previous two steps of these instructions.

   You can write identical geographic data attributes to different event fields. If you configure multiple geographic data attributes to be written to the same event field, the event will be enriched with the last mapping in the sequence.

Assets

This enrichment method lets you find an asset based on values of normalized event fields. If a matching asset is found, the `AssetID` is written to the specified event field.

Settings of the "Assets" enrichment type

Setting	Description
Raw event field	Normalized event field whose value is used to look up the corresponding asset in the KUMA database. Fields can be used to match an asset include `DeviceAddress`, `DeviceHostName`, `SourceAddress`, `SourceHostName`, `DestinationAddress`, `DestinationHostName`.
Target event field	The event field to which the ID of the found asset (`AssetID`) is written. The available fields are `SourceAssetID`, `DeviceAssetID`, and `DestinationAssetID`.

When enrichment is performed, the value from the **Source event field** is compared with the asset details. If they match, the ID of the found asset is written to the **Target event field** If no matching asset is found, the target field is left empty.

Accounts

This enrichment method looks up a user account by the values of the event fields and the attributes of the user account. This rule allows you to match event data against user accounts from the directory and write the `AccountID` of the found user account to the event.

Settings of the "User accounts" enrichment type

Setting	Description
Target event field	The normalized event field to which the `AccountID` of the found user account is recorded. The available fields are `SourceAccountID` and `DestinationAccountID`.
Domain event field	The event field that contains the name of the domain in which to search for the user account. If the field value is not specified, the search is performed in all domains specified in the rule.
Mapping	The set of mappings between event fields and user account attributes. An event field value is compared with its corresponding user account attribute. To add a mapping, click the **Add** button and specify the following: • **Event field**, the event field whose value is used for searching. • **User account field**, the attribute of the user account with which the value of the event field is compared.

If a user account is found, its `AccountID` is written to the **Target event field**. If multiple mappings are specified in a rule, they are evaluated sequentially until a match is found.

5. If necessary, in the **Tags** drop-down list, select thetags for the enrichment rule.

6. If required, add a description for the enrichment rule in the **Description** field.

7. Under **Selector**, you can specify conditions to identify events that will be processed using the enrichment rule. You can enter this condition manually on the **Code** tab or build it on the **Builder** tab.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

8. Then click the **Create** button.

The new enrichment rule was added to the resource set for the correlator.

4 Adding a response rule

You can create response rules and indicate which actions must be performed when the correlation rules are triggered. There can be multiple response rules. You can add these by clicking the **Add** button and can remove them by clicking the **Delete** button.

To add a response rule:

1. In the **Response** section, click the **Add** button.

2. In the **Name** field, enter a unique name for the response rule. The name must contain 1 to 128 Unicode characters.

3. In the **Tenant** drop-down list, select the tenant that you want to own the response rule.

4. In the **Type** drop-down list, select the type of response rule and define its corresponding settings:

   - **Response via KSC**—response rules for automatically launching the tasks on Kaspersky Security Center assets. For example, you can configure automatic startup of a virus scan or database update.

     Tasks are automatically started when KUMA is integrated with Kaspersky Security Center. Tasks are run only on assets that were imported from Kaspersky Security Center.

     Response settings

     - **Kaspersky Security Center task** (required)—name of the Kaspersky Security Center task that you need to start. Tasks must be created beforehand, and their names must begin with "`KUMA `". For example, "`KUMA antivirus check`".

       Types of Kaspersky Security Center tasks that can be started using KUMA:

       - Update

       - Virus scan

- **Event field** (required)—defines the event field of the asset for which the Kaspersky Security Center task should be started. Possible values:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

> To send requests to Kaspersky Security Center, you must ensure that Kaspersky Security Center is available over the UDP protocol.

- **Run script**—response rules for automatically running a script. For example, you can create a script containing commands to be executed on the KUMA server when selected events are detected.

  The script file is stored on the server where the correlator service using the response resource is installed: /opt/kaspersky/kuma/correlator/<correlator ID>/scripts.

  The `kuma` user of this server requires the permissions to run the script.

  Response settings

  - **Timeout**—the number of seconds the system will wait before running the script.
  - **Script name** (required)—the name of the script file.

    If the script Response resource is linked to the Correlator service, but the is no script file in the /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts directory, the service will not start.
  - **Script arguments**—parameters or correlation event field values that must be passed to the script.

    > If the script includes actions taken on files, you should specify the absolute path to these files.

    Parameters can be written with quotation marks (").

    Correlation event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field which value must be passed to the script.

    Example: `-n "\"usr\": {{.SourceUserName}}"`

- **Response via KEDR**—response rules for automatically creating prevention rules, starting network isolation, or starting the application on Kaspersky Endpoint Detection and Response and Kaspersky Security Center assets.

  Automatic response actions are carried out when KUMA is integrated with Kaspersky Endpoint Detection and Response.

  Response settings

  - **Event field** (required)—event field containing the asset for which the response actions are needed. Possible values:
    - **SourceAssetID**
    - **DestinationAssetID**
    - **DeviceAssetID**

- **Task type**—response action to be performed when data matching the filter is received. The following types of response actions are available:

  - **Enable network isolation**.

    When selecting this type of response, you need to define values for the following settings:

    - **Isolation timeout**—the number of hours during which the network isolation of an asset will be active. You can indicate from 1 to 9,999 hours.

      If necessary, you can add an exclusion from network isolation.

      How to add an exclusion from network isolation

      To add an exclusion for network isolation:

      a. Click the **Add exclusion** button.

      b. Select the direction of network traffic that must not be blocked:

      - Inbound.
      - Outbound.
      - Inbound/Outbound.

      c. In the **Asset IP** field, enter the IP address of the asset whose network traffic must not be blocked.

      d. If you selected **Inbound** or **Outbound**, specify the connection ports in the **Remote ports** and **Local ports** fields.

      e. If you want to add more than one exclusion, click **Add exclusion** and repeat the steps to fill in the **Traffic direction**, **Asset IP**, **Remote ports** and **Local ports** fields.

      f. If you want to delete an exclusion, click the **Delete** button under the relevant exclusion.

      > When adding exclusions to a network isolation rule, Kaspersky Endpoint Detection and Response may incorrectly display the port values in the rule details. This does not affect application performance. For more details on viewing a network isolation rule, please refer to the *Kaspersky Anti Targeted Attack Platform Help Guide*.

  - **Disable network isolation**.

  - **Add prevention rule**.

    When selecting this type of response, you need to define values for the following settings:

    - **Event fields to extract hash from**—event fields from which KUMA extracts SHA256 or MD5 hashes of the files that must be prevented from starting.

      > The selected event fields and the values selected in the **Event field** must be added to the inherited fields of the correlation rule.

    - **File hash #1**—SHA256 or MD5 hash of the file to be blocked.

At least one of the above fields must be completed.

- **Delete prevention rule**.
- **Run program**.

  When selecting this type of response, you need to define values for the following settings:

  - **File path**—path to the file of the process that you want to start.
  - **Command line parameters**—parameters with which you want to start the file.
  - **Working directory**—directory in which the file is located at the time of startup.
  - **Hosts**—hosts on which the specified application is to be executed.

  When a response rule is triggered for users with the General Administrator role, the **Run program** task will be displayed in the **Task manager** section of the application web interface. In the **Created by** column of the task table, **Scheduled task** is displayed for this task . You can view task completion results.

  All of the listed operations can be performed on assets that have Kaspersky Endpoint Agent for Windows. On assets that have Kaspersky Endpoint Agent for Linux, the application can only be started.

  At the software level, the capability to create prevention rules and network isolation rules for assets with Kaspersky Endpoint Agent for Linux is unlimited. KUMA and Kaspersky Endpoint Detection and Response do not provide any notifications about unsuccessful application of these rules.

- **Response via KICS/KATA**—response rules for automatically starting tasks on KICS for Networks assets. For example, you can change the asset status in KICS for Networks.

  Tasks are automatically started when KUMA is integrated with KICS for Networks.

  Response settings

  - **Event field** (required)—event field containing the asset for which the response actions are needed. Possible values:
    - **SourceAssetID**
    - **DestinationAssetID**
    - **DeviceAssetID**
  - **Status of the asset in KICS/KATA** is the status to be set for the specified asset. The following values are available:
    - **Unauthorized**
    - **Authorized**

When a response rule is triggered, KUMA will send KICS/KATA an API request to change the status of the specified asset to the selected status.

- **Response via Active Directory**—response rules for changing the permissions of Active Directory users. For example, block a user.

  Tasks are started if integration with Active Directory is configured.

  Response settings

  - **Account ID source** is the event field from which the value of the Active Directory account ID is taken. Possible values:
    - **SourceAccountID**
    - **DestinationAccountID**
  - **AD command**—command that is applied to the account when the response rule is triggered. Available values
    - **Add account to group**
    - **Remove account from group**
    - **Reset account password**
    - **Block account**.

5. Under **Selector**, you can specify conditions to identify events that will be processed using the response rule. You can enter this condition manually on the **Code** tab or build it on the **Builder** tab.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

6. Then click the **Create** button.

The new response rule was added to the resource set for the correlator.

5 Adding a destination

You can create destinations with settings indicating the forwarding destination for events created by the correlator. Events from a correlator are usually redirected to a storage so that they can be saved and viewed later if necessary. Events can be sent to other locations as needed. There can be more than one destination point.

To add a destination:

1. In the **Routing** section, click the **Add** button.

2. On the **Basic settings** tab, specify the following settings:

   a. In the **Name** field, enter a unique name for the destination. The name must contain 1 to 128 Unicode characters.

   b. In the **Tenant** drop-down list, select the tenant that you want to own the destination.

c. You can use the **State** toggle switch to enable or disable the destination as needed.

d. In the **Destination type** drop-down list, select the type of the destination. The following values are available:

- **Storage**.
- **Internal**.
- **Correlator**.

e. In the **URL** field, specify the URL that you want to connect to. The following URL formats are supported:

- `<host name>:<port number>`
- `<IPv4 address>:<port number>`
- `<IPv6 address>:<port number>`
- You can specify IPv6 addresses in the following format: `[<IPv6 address>%<interface>:<port number>`, for example, `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`.

You can add or remove multiple URLs. Kaspersky SIEM does not allow saving a resource or service if the **URL** field contains a tab or space character. To add a URL, click the **Add URL** button. To remove a URL, click the trash can 🗑 icon next to it.

f. In the **Path** field, specify the path that you want to add to the request to the URL specified in the **URL** field. For example, if you specify `/input` as the path and enter `10.10.10.10` for the URL, the destination will make requests to `10.10.10.10/input`.

g. If necessary, in the **Tags** field, specify the tags to help find the destination.

h. If necessary, enter a description of the destination in the **Description** field. The maximum length of the description is 4000 Unicode characters.

i. Under **Selector**, you can set the conditions for determining which events are to be sent to the destination. You can enter this condition manually on the **Code** tab or build it on the **Builder** tab.

When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved.

3. On the **Advanced settings** tab, specify the following settings:

a. In the **URL selection policy** drop-down list, select the method for determining the priority of URLs to which events are sent, if you have added multiple URLs to the **URL** field on the **Basic settings** tab:

- **Prefer first** means events are sent to the first added URL. If the URL becomes unavailable, events are sent to the next available added URL. If the first added URL becomes available again, events are sent to the first added URL again.
- **Round robin** means events are evenly balanced among the available URLs. This method does not guarantee that events are evenly balanced among the URLs because the buffer may overflow or events may be sent to the destination. You can specify the buffer size in bytes in the **Buffer size limit** field; you can also specify the interval in seconds for sending events to the destination in the **Buffer flush interval** field.

b. In the **Timeout** field, enter the time in seconds, for which the destination waits for a response from another service or component.

c. In the **Health check path** field, enter the URL for sending requests to get information about the health of the system that the destination resource is connecting to.

d. In the **Health check timeout** field, enter the interval in seconds for checking the health of the destination.

e. In the **Buffer size** field, enter the size in bytes of the buffer for accumulating events in the RAM of the server before sending them for further processing or storage. The value must be a positive integer. The default buffer size is 1,048,576 bytes.

f. In the **Buffer flush interval** field, specify the interval in seconds for sending events to the destination. The default value is 1 second.

g. In the **Workers** field, specify the number of workers that the service can run simultaneously to process events in parallel. The default value is 64.

h. If necessary, enable the disk buffer using the **Disk buffer** toggle switch. This toggle switch is turned on by default.

   The disk buffer is used if the collector cannot send normalized events to the destination. You can specify the size of the disk buffer in the **Disk buffer size limit** field. If the disk buffer runs out of free space, new normalized events will overwrite old normalized events, starting with the oldest.

i. In the **Disk buffer size limit** field, specify the size of the disk buffer in bytes. The default value is 10,737,418,240 bytes (10 GB).

j. In the **Maximum disk buffer segments** field, specify the maximum number of segments into which the disk buffer can be divided. The default value is 10.

k. In the **Disk buffer drain interval (sec)** field, specify the interval in seconds between operations disk buffer flushes to send the events onwards. The default value is 5 seconds.

l. In the **Disk buffer fsync interval (sec)** field, specify the interval in seconds between `fsync` operations for writing disk buffer data to disk. The default value is 1 second.

m. In the **Disk buffer cursor sync interval (sec)**, specify the interval in seconds between disk buffer read position (cursor) synchronization operations. The default value is 1 second.

4. Then click the **Create** button.

The new destination is added to the resource set for the correlator.

6 Testing correlator settings

At this stage, KUMA creates a service resource set with the services being created automatically based on this set:

- The set of resources for the correlator is displayed in the **Resources** → **Correlators** → **NG** section. It can be used to create new correlator services. When this set of resources changes, all services that operate based on it will start using the new parameters after the services restart. To do so, you can use the **Save and restart services** and **Save and update service configurations** buttons.

  A resource set can be modified, copied, moved from one folder to another, deleted, imported, and exported, like other resources.

- Services are displayed in **Resources** → **Active services**. The services created using the Installation Wizard perform functions inside the KUMA solution. To communicate with external parts of the network infrastructure, you need to install similar external services on the servers and assets intended for them. For example, an external correlator service should be installed on a server intended to process events, external storage services should be installed on servers with a deployed ClickHouse service, and external agent services should be installed on Windows assets that must both receive and forward Windows events.

To test correlator settings:

1. Click **Create and save service**.

   The **Setup validation** section displays a table of services created based on the set of resources selected in the Installation Wizard. The lower part of the window shows examples of commands that you must use to install external equivalents of these services on their intended servers and assets.

   Example

   ```
   sudo /opt/kaspersky/kuma/kuma ng correlator --id <service_ID> --core https://<FQDN>:<port> --api.port
   <API_port> --wd
   sudo /opt/kaspersky/kuma/correlatorNg/<UUID> --pair.fingerprint <CA_certificate_ID>
   ```

   where:

   `<service_ID>` is the ID of the service.

   `<FQDN>` is the fully qualified domain name of KUMA Core server.

   `<port>` is the port used for communication with the KUMA Core.

   `<API_port>` is the port used for communication with the service.

   `<UUID>` is the unique ID of the correlator.

   `<CA_certificate_ID>` is the fingerprint ID of the KUMA Core CA certificate.

   The port for communication with the KUMA Core, the service ID, the ID of the CA certificate, the port for communication with the service, and the unique ID of the correlator are added to the command automatically. You should also ensure the network connectivity of the KUMA system and open the ports used by its components if necessary.

2. Close the correlator creation window by clicking **Create**.

After finishing creating and configuring the correlator, you need to install the KUMA correlator on the server using the command copied from the **Setup validation** section.

Supported data types for correlator NG

KUMA 4.6 introduces a beta version of correlator-ng for technical reference. Methods, algorithms, syntax of conditions, and other functions and characteristics may change before the release of the fully functional version of the correlator API.

Correlator-ng has a stricter data model compared to the standard version of the correlator. This affects correlation rules, selectors, and event processing functions. Each field of an event, variable, or selector now has a defined type. Automatic type casting is used only for compatible types; in other cases, the `to_string`, `to_integer`, and `to_float` conversion functions must be used.

The following data types are supported:

Supported data types

Data type	Description
String	String
VecString	Array of strings
I64	64-bit integer
VecI64	Array of 64-bit integers
F64	Float
VecF64	Array of floats
Timestamp	UNIX Timestamp (in milliseconds)
VecTimestamp	Array of UNIX Timestamps (in milliseconds)
Uuid	Unique ID in the UUIDv4 format
VecUuid	Array of UUIDv4 values
Ip	IPv4 or IPv6 address
VecIp	Array of IP addresses
IpNet	Subnet with a CIDR prefix, for example, `192.168.1.0/24`.
VecIpNet	Array of subnets
Bool	Boolean value (`true` or `false`)
VecBool	Array of boolean values.

Stronger typing improves the efficiency of the correlator and reduces errors when compiling correlation rules. However, all operations with arrays, strings and timestamps must now take into account the data type, otherwise runtime errors can occur.

Correlation rule selectors and expressions

KUMA 4.6 introduces a beta version of correlator-ng for technical reference. Methods, algorithms, syntax of conditions, and other functions and characteristics may change before the release of the fully functional version of the correlator API.

In correlator-ng, selectors can do all that variables can, and can use functions for working with strings, arrays, and numbers (for example, `substring`, `tr`, `to_lower`). It is not necessary to create a separate variable to use functions; the selectors themselves can use these functions.

Selectors are described using the SQL syntax applicable to `WHERE` clauses.

Selectors and variables are configured using expressions for filtering and merging events. They support the same operations as variables, with the ability to construct sophisticated conditions. The following expression types are available.

> When writing expressions for comparing values that involve constants, the constant must go on the right. This lets the correlator apply various optimizations. If the constant is in the left part, no optimization is done.

Constants

Constants

Constant	Type
`1`	I64 (integer)
`3.14`	F64 (float)
`'myString'`	String

References to values

References to values

Reference	Description
`DeviceVendor`	Value of `DeviceVendor` event field
`S.MyCustomField`	Value of `S.MyCustomField` composite field
`$myVariable`	Value of `myVariable` variable

Logical and group operators

Logical and group operators

Expression	Description
`<expression> AND <expression>`	Logical AND operator
`<expression> OR <expression>`	Logical OR operator
`NOT <expression>`	Negation of the result of an expression
`IS [NOT] NULL`	Checking for the absence of a value (in correlator-ng, an unset value is `NULL`)
`()`	Grouping expressions

Comparison operators

Comparison operators

Expression	Description
`<expression> = <expression>`	Checks for equality of values
`<expression> > <expression>`	Compares values using the `>` operator
`<expression> >= <expression>`	Compares values using the `>=` operator
`<expression> < <expression>`	Compares values using the `<` operator
`<expression> <= <expression>`	Compares values using the `<=` operator
`Type BETWEEN 1 AND 3`	Checks if the value of the `Type` field is between 1 and 3 inclusive

Arithmetic operators

Arithmetic operators

Expression	Description
`<expression> + <expression>`	Addition
`<expression> - <expression>`	Subtraction
`<expression> * <expression>`	Multiplication
`<expression> / <expression>`	Division
`<expression> % <expression>`	Modulo division

Features

Features

Function	Description
`eq_fold (<left operand expression>, <right operand expression>)`	Calls the `eq_fold` function.

For details about the available functions, see the Data processing functions in correlator-ng section.

Data processing functions in correlator NG

KUMA 4.6 introduces a beta version of correlator-ng for technical reference. Methods, algorithms, syntax of conditions, and other functions and characteristics may change before the release of the fully functional version of the correlator API.

Functions in correlator-ng are used in selectors and variables for working with event data, type casting, and filtering.

General syntax:

- Required arguments are enclosed in `< >`, optional arguments are enclosed in `[ ]`.
- Three dots `...` stand for an indefinite number of arguments.
- The return type is denoted by `-> <data type>`. The letter `T` indicates that the type depends on the type of the arguments.
- The type of the arguments can be concrete (for example, `String`, `I64`) or `T`, which stands for any available data type.

Type casting functions

These functions cast a value to a certain type.

Type casting functions

Function	Description
`to_string(< expression >)`	Casts the value to string.
`to_integer(< expression >)`	Casts the value to integer (I64).
`to_float(< expression >)`	Casts the value to float (F64).
`to_uuid(< expression >)`	Casts the value to UUIDv4.
`to_ip(< expression >)`	Casts the value to IPv4 or IPv6 address.
`to_ip_net(< expression >)`	Casts the value to an IPNet subnet.
`to_bool(< expression >)`	Casts the value to boolean.
`to_timestamp(< expression >, '[ timezone ]')`	Casts the value to a timestamp with an optional timezone.

Functions for comparing values

Functions for comparing values

Function	Description
`eq_fold(< left_operand >, < right_operand >) -> Bool`	Checks if the left-side value is the same as the right-side value, ignoring case.
`eq_any(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks if one of the right-side values is the same as the left-side value.
`eq_any_fold(< left_operand >, < right_operand >, [...]) -> Bool`	Compares the left-side value with multiple right-side values, ignoring case.
`contains(< left_operand >, < right_operand >) -> Bool`	Checks if the left-side value contains the right-side value.
`contains_fold(< left_operand >, < right_operand >) -> Bool`	Checks if the left-side value contains the right-side value, ignoring case.
`contains_any(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks if the left-side value contains any of the right-side values.
`contains_any_fold(< left_operand >, < right_operand >, [...]) -> Bool`	Checks if the left-side value contains any of the right-side values, ignoring case.
`starts_with(< left_operand >, < right_operand >) -> Bool`	Checks if the right-side value is a prefix of the left-side value.

Function	Description
`starts_with_fold(< left_operand >, < right_operand >) -> Bool`	Checks the prefix, case-insensitive.
`starts_with_any(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks if one of the right-side values is a prefix of the left-side value.
`starts_with_any_fold(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks the prefix for one of the right-side values, case-insensitive.
`ends_with(< left_operand >, < right_operand >) -> Bool`	Checks if the right-side value is a suffix of the left-side value.
`ends_with_fold(< left_operand >, < right_operand >) -> Bool`	Checks the suffix, case-insensitive.
`ends_with_any(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks if one of the right-side values is a suffix of the left-side value.
`ends_with_any_fold(< left_operand >, < right_operand 1>, [...]) -> Bool`	Checks the suffix, case-insensitive.
`match(< left_operand >, < right_operand >) -> Bool`	Checks if the left-side value matches the regular expression on the right side.
`match_any(< left_operand >, '< right_operand 1>', '[ right_operand 2]', [...]) -> Bool`	Checks if the left-side value matches one of the regular expressions on the right side.

Functions for working with active lists, dictionaries, and context tables

Functions for working with active lists, dictionaries, and context tables

Function	Description
`in_active_list('< active_list_ID >', < key_element 1>, [...]) -> Bool`	Checks for the presence of a value in the active list by key.
`in_context_table('< context_table_ID >', '< key_field_name 1>', < key_field_value 1>, '[ key_field_name 2]', [ key_field_value 2], [...]) -> Bool`	Checks for the presence of a value in the context table by key.
`in_dictionary('< dictionary_ID >', < key_element 1>, [ key_element 2], ...) -> Bool`	Checks for the presence of a value in the dictionary by key.
`dict('< dictionary_ID >', < key 1>, [...]) -> String`	Returns a value from a dictionary by key.
`table_dict('< dictionary_ID >', < column_name >, < key 1>, [...]) -> String`	Returns a value from a table dictionary.
`active_list('< active_list_ID >', < field_name >, < key 1>, [...]) -> String`	Returns a value from an active list.
`context_table('< context_table_ID >', '< field_name >', '< key_field >', < value >) -> T`	Returns the value of a field from the context table.
`context_table_list_item('< context_table_ID >', '< field_name >', < index >, ...) -> T`	Returns an array element from a context table.
`match_active_list(...)`	Returns a value from an active list if the key matches a regular expression.
`match_context_table(...)`	Returns a value from a context table if a regular expression is matched.
`match_dictionary(...)`	Returns a value from a dictionary if a regular expression is matched.

Subnet functions

Subnet functions

Function	Description
`in_subnet(< left_operand >, < subnet >) -> Bool`	Checks if an IP address belongs to a subnet.
`in_subnet_any(< left_operand >, < subnet 1>, [...]) -> Bool`	Checks if an IP address belongs to one of the subnets.
`in_subnet_active_list(...)`	Checks if an IP address belongs to a subnet from an active list.
`in_subnet_context_table(...)`	Checks if an IP address belongs to a subnet from a context table.
`in_subnet_dictionary(...)`	Checks if an IP address belongs to a subnet from a dictionary.

String functions

String functions

Function	Description
`to_lower(< operand >) -> String`	Converts the string to lower case.
`to_upper(< operand >) -> String`	Converts the string to upper case.
`substring(< string >, < beginning_of_substring >, [ end_of_substring ]) -> String`	Returns a substring.
`index_of(< find_what >, < find_where >) -> I64`	Returns the position of the first occurrence.
`last_index_of(< find_what >, < find_where >) -> I64`	Returns the position of the last occurrence.
`tr(< operand >) -> String`	Trims whitespace at the beginning and end of a string.
`replace(< string >, < substring >, < replacement >) -> String`	Replaces a substring.
`regexp_replace(< string >, '< regular_expression >', '< replacement >') -> String`	Replaces a substring using a regular expression.
`regexp_capture(< string >, '< regular_expression >') -> String`	Gets a substring matching a regular expression.
`str_join('< separator >', < string 1>, [...]) -> String`	Joins multiple strings.

Array functions

Array functions

Function	Description
`append(< left operand >, < right operand >, '[ separator ]') -> T`	Adds a value to the end of an array or string.
`prepend(< left operand >, < right operand >, '[ separator ]') -> T`	Adds a value to the beginning of an array or string.
`len(< operand >) -> I64`	Returns the length of a string or array.
`item(< array >, < index >) -> T`	Returns an element of an array by index.
`distinct_items(< array >) -> T`	Removes duplicate elements from an array.
`sort_items(< array >, '< sorting_order >') -> T`	Sorts an array.

Timestamp functions

Timestamp functions

Function	Description
`now() -> Timestamp`	Returns the current timestamp.
`year(<timestamp>) -> I64`	Returns the year.
`month(<timestamp>) -> I64`	Returns the month number.
`month_str(<timestamp>) -> String`	Returns the month in string form.
`weekday(<timestamp>) -> I64`	Returns the number of the day of the week.
`weekday_str(<timestamp>) -> String`	Returns the day of the week in string form.
`day(<timestamp>) -> I64`	Returns the day of the month.
`hour(<timestamp>) -> I64`	Returns the hour.
`minute(<timestamp>) -> I64`	Returns the minute.
`second(<timestamp>) -> I64`	Returns the second.
`millisecond(<timestamp>) -> I64`	Returns the millisecond.
`format_timestamp(<timestamp>, '< format >') -> String`	Converts the timestamp to a string.
`truncate_timestamp(<timestamp>, '< duration >') -> Timestamp`	Rounds the timestamp to an integer value.

Time functions

Time functions

Function	Description
`duration_days(<t1>, <t2>) -> I64`	Returns the difference in days.
`duration_hours(<t1>, <t2>) -> I64`	Returns the difference in hours.
`duration_minutes(<t1>, <t2>) -> I64`	Returns the difference in minutes.
`duration_seconds(<t1>, <t2>) -> I64`	Returns the difference in seconds.
`duration_milliseconds(<t1>, <t2>) -> I64`	Returns the difference in milliseconds.

Mathematical functions

Mathematical functions

Function	Description
`round(< operand >) -> I64`	Rounds the value to the nearest integer.
`ceil(< operand >) -> I64`	Rounds the value up.
`floor(< operand >) -> I64`	Rounds the value down.
`abs(< operand >) -> T`	Returns the absolute value of a number.
`pow(< operand >, '< power >') -> T`	Raises a number to a power.
`math_min(< array >) -> T`	Returns the minimum element of an array.

Function	Description
`math_max(< array >) -> T`	Returns the maximum element of an array
`math_avg(< array >) -> F64`	Calculates the average value of an array.

Data decoding and analysis functions

Data decoding and analysis functions

Function	Description
`decode_hex_integer(< string >) -> I64`	Converts a hex string to a number.
`decode_hex(< string >) -> String`	Decodes a hex string.
`decode_base64(< string >) -> String`	Decodes a Base64 string.
`decode_url(< string >) -> String`	Decodes a URL-encoded string.
`entropy(< string >) -> F64`	Calculates the Shannon entropy of a string.
`has_bit(< left_operand >, < position >) -> Bool`	Checks if the bit is set at the specified position.
`has_vulnerability(< asset_ID >, (<CVE>), [ severity ]) -> Bool`	Checks if an asset has a vulnerability.

Other functions

Other functions

Function	Description
`include('< predicate_ID >', '[ predicate_name ]')`	Uses predefined predicates from the selector-includes.yaml file.
`ti('< category >', < indicator >, '< field >')`	Retrieves a value from a specialized TI field (CyberTrace).
`with_selector(' correlation_rule_selector_tag ', < expression >)`	Can only be used in the `joinSelector` attribute of a correlation rule to distinguish between sets of events.
`template('< template >', [ argument 1], [ argument 2], ...) -> String`	Generates a string based on a template by interpolating the values of event fields or variables into it.
`conditional('< predicate >', <then>, <else>)`	Returns one of two values, depending on the result of the predicate
`has_ti_detect*()`	Checks for a CyberTrace triggering by category or indicator.
`has_ti_detect_with_category('< category >')`	Checks for a CyberTrace triggering by category.
`has_ti_detect_with_indicator(< indicator >)`	Checks for a CyberTrace triggering by indicator.
`has_ti_detect_with_category_and_indicator('< category >', < indicator >)`	Checks for a CyberTrace triggering by category and indicator.

Installing the correlator on the server

After creating a correlator, install it on a server in the network infrastructure used to receive events.

To install a correlator:

1. Log in to the server where you want to install the service.

2. Run the command that you copied at the last stage of creating the correlator, **Setup validation**.

```
Example command for installing a standard correlator

sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <CA_certificate_ID> --
id <service_ID> --api.port <API_port> --install
```

```
Example of a command for installing an NG correlator

sudo /opt/kaspersky/kuma/kuma ng correlator --id <service_ID> --core https://<FQDN>:<port> --api.port
<API_port> --wd
sudo /opt/kaspersky/kuma/correlatorNg/<UUID> --pair.fingerprint <CA_certificate_ID>
```

The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

> When deploying several KUMA services on the same host, during the installation process you must specify unique ports for each component using the `--api.port <API_port>` option. The following setting values are used by default: `--api.port 7221`.

The correlator is installed. You can use it to analyze events for threats.

To check if the correlator is ready to receive events:

1. In the KUMA web interface, open **Resources** → **Active services**.

2. Make sure that the correlator you installed has the green status.

If the events that are fed into the correlator contain events that meet the correlation rule filter conditions, the events tab will show events with the `DeviceVendor=Kaspersky` and `DeviceProduct=KUMA` parameters. The name of the triggered correlation rule will be displayed as the name of these correlation events.

If no correlation events are found, you can create a simpler version of your correlation rule to find possible errors. Use a correlation rule of the **Simple** type and a single **Output** action. It is recommended to create a filter to find events that are regularly received by KUMA.

When updating, adding, or removing a correlation rule, you must update configuration of the correlator.

> When you finish testing your correlation rules, you must remove all testing and temporary correlation rules from KUMA and update configuration of the correlator.

Correlation rules

Correlation rules are used to recognize specific sequences of processed events and to take certain actions after recognition, such as creating correlation events/alerts or interacting with an active list.

To learn more about the basics of correlation rules, watch the video below, and then follow the step-by-step instructions for managing correlation rules.

https://www.youtube.com/watch?v=G2F0I7SZG6Q

Correlation rules can be used in the following KUMA services and features:

- Correlator.
- Notification rule.
- Links of segmentation rules.
- Retrospective scan.

The available correlation rule settings depend on the selected type. Types of correlation rules:

- standard is used to find correlations between several events. Resources of this kind can create correlation events.

  This rule kind is used to determine complex correlation patterns. For simpler patterns you should use other correlation rule kinds that require less resources to operate.

- simple is used to create correlation events if a certain event is found.
- operational is used for operations with active lists and context tables. This rule kind cannot create correlation events.

For these resources, you can enable the display of control characters in all input fields except the **Description** field.

If a correlation rule is used in the correlator and an alert was created based on it, any change to the correlation rule will not result in a change to the existing alert even if the correlator service is restarted. For example, if the name of a correlation rule is changed, the name of the alert will remain the same. If you close the existing alert, a new alert will be created and it will take into account the changes made to the correlation rule.

If a correlation rule uses a different resource, for example, a previously saved filter, and this resource is modified, then if the correlation rule exported to a file may contain data from an earlier version of the modified resource. However, subsequent import of the correlation rule from this file is completed correctly, and KUMA imports the latest version of the resource.

Working with correlation rules

You can create, copy, modify, and delete correlation rules.

To learn more about creating a correlation rule, watch the video below, and then follow the step-by-step instructions.

[▷]

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

Creating a correlation rule

To create a correlation rule:

1. In the web interface, open the **Resources** → **Correlation rules** section and click the **Create** button.

   The correlation rule creation pane opens on the right.

2. In the **General** tab, perform the following actions:

   a. Enter a resource name in the **Name** field. The resource name must be unique within the selected tenant.

   b. In the **Tenant** drop-down list, select the tenant to which the correlation rule to be applied.

c. In the **Type** drop-down list, select the type of correlation rule: **standard**, **simple**, or **operational**.

d. If necessary, add tags from the **Tags** drop-down list.

e. Specify the triggering frequency of the correlation rule.

f. If necessary, add a description for the correlation rule.

g. In the **MITRE techniques** drop-down list, select the threat detection techniques to be applied in the correlation rule.

3. On the **Selectors** tab, specify the conditions for triggering the correlation rule. To do so:

   - In the **Settings** tab, perform one of the following actions:

     - In the **Filter** drop-down list, select or create a filter to define the event that triggers the correlation rule.

       To save the selected filter, select the **Save filter** check box.

     - Use the builder to specify the triggering condition for the correlation rule (see examples).

     - Enter the condition code for triggering the correlation rule.

   - If necessary, on the **Local variables** tab, specify the local variables for the rule triggering condition.

4. On the **Actions** tab, add resource update operations.

5. Click **Create**.

Correlation rule will be created and available for use in services and other resources.

Copying a correlation rule

To copy a correlation rule:

1. In the web interface, open the **Resources** → **Correlation rules** section and select the check box next to the correlation rule that you want to copy.

2. Click **Duplicate**.

   This will display the number of selected rules in the lower part of the table.

   On the right, a pane with the parameters of the correlation rule that you have selected for copying opens.

   The **Name** field displays a `<name of the selected correlation rule> - copy`.

3. Change the required parameters (see the instructions for creating a correlation rule).

4. Click **Save**.

A copy of the correlation rule is created.

Editing the settings of a correlation rule

To change a correlation rule:

1. In the web interface, open the **Resources** → **Correlation rules** section and click the rule that you want to edit.

   On the right, a pane with the parameters of the selected correlation rule opens.

2. Change the required parameters (see the instructions for creating a correlation rule).

3. Do one of the following:

   - Click **Save** to save your changes.

   - Click **Save with comment**, and in the window that opens add a comment that describes your changes. The changes will be saved and the comment will be added to the created version of the correlation rule.

   If, when saving changes, it turns out that the current version of a correlation rule has been modified by another user, you are prompted to select one of the following actions:

   - Save your changes as a new version on top of the changes made by another user.

   - Save your changes as a new correlation rule.

     In this case, a duplicate of the original correlation rule is created with changed settings. The `- copy` part is added to the name of a new rule, and the name and version of the resource that was duplicated is specified in the comments for the correlation rule version.

   - Discard your changes.

     Discarded changes cannot be restored.

   The correlation rule will be updated. If this resource is used in a service, restart the service so that it uses the new correlation rule version.

Deleting a correlation rule

To delete a correlation rule:

1. In the web interface, open the **Resources** → **Correlation rules** section and select the check box next to the correlation rule that you want to delete.

   The number of selected resources is displayed in the lower part of the table.

2. Click **Delete**.

3. In the window that opens, confirm the deletion.

   The correlation rule and all its saved versions will be deleted.

Correlation rules of the 'standard' type

Correlation rules of the **standard** type are used for identifying complex patterns in processed events.

The search for patterns is conducted by using buckets

Bucket is a data container that is used by the Correlation rule resources to determine if the correlation event should be created. It has the following functions:

- Group together events that were matched by the filters in the **Selectors** group of settings of the Correlation rule resource. Events are grouped by the fields that were selected by user in the **Identical fields** field.
- Determine the instance when the Correlation rule should trigger, affecting the events that are grouped in the bucket.
- Perform the actions that are selected in the **Actions** group of settings.
- Create correlation events.

Available states of the Bucket:

- `Empty`—the bucket has no events. This can happen only when it was created by the correlation rule triggering.
- `Partial Match`—the bucket has some of the expected events (recovery events are not counted).
- `Full Match`—the bucket has all of the expected events (recovery events are not counted). When this condition is achieved:
  - The Correlation rule triggers
  - Events are cleared from the bucket
  - The trigger counter of the bucket is updated
  - The state of the bucket becomes `Empty`
- `False Match`—this state of the Bucket is possible:
  - when the `Full Match` state was achieved but the join-filter returned false.
  - when **Recovery** check box was selected and the recovery events were received.

  When this condition is achieved the Correlation rule does not trigger. Events are cleared from the bucket, the trigger counter is updated, and the state of the bucket becomes `Empty`.

In comparison with the data model of the normalized event, some fields of the correlation event formed by the **standard** correlation rule may be different (see the table below).

Name of the correlation event field	Description
StartTime	The earliest base event creation date and time (timestamp) among all base events from which the correlation event was generated.
EndTime	The later of the following dates and times: • Date and time when the correlation event was created. • The latest base event creation date and time (timestamp) among all base events from which the correlation event was generated.

To add fields from base events to the correlation event, specify these fields in the **Identical fields** and **Unique fields** parameters (see the table below).

Settings for a correlation rule of the **standard** type are described in the following tables.

General tab

This tab lets you specify the general settings of the correlation rule.

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Correlation rule type: **standard**. Required setting.
Tags	Tags for resource search. Optional setting.
Identical fields	Event fields that must be grouped in a Bucket. The hash of the values of the selected event fields is used as the Bucket key. If one of the selectors specified on the **Selectors** tab is triggered, the selected event fields are copied to the correlation event. If different selectors of the correlation rule use event fields that have different meanings in the events, do not specify such event fields in the **Identical fields** drop-down list. You can specify local variables. To refer to a local variable, its name must be preceded with the `$` character. For an example of using local variables, refer to the rule provided with KUMA: **R403_Access to malicious resources from a host with disabled protection or an out-of-date anti-virus database**. Required setting.
Window, sec	Bucket lifetime in seconds. The time starts counting when the bucket is created, when the bucket receives the first event. When the bucket lifetime expires, the trigger specified on the **Actions** → **On timeout** tab is triggered, and the container is deleted. Triggers specified on the **Actions** → **On every threshold** and **On subsequent thresholds** tabs can trigger more than once during the lifetime of the bucket. Required setting.
Unique fields	Unique event fields to be sent to the bucket. If you specify unique event fields, only these event fields will be sent to the container. The hash of values of the selected fields is used as the Bucket key. You can specify local variables. To refer to a local variable, its name must be preceded with the `$` character. For an example of using local variables, refer to the rule provided with KUMA: **R403_Access to malicious resources from a host with disabled protection or an out-of-date anti-virus database**.
Rate limit	Maximum number of times a correlation rule can be triggered per second. The default value is `0`. If correlation rules employing complex logic for pattern detection are not triggered, this may be due to the way rule triggers are counted in KUMA. In this case, we recommend increasing the **Rate limit**, for example, to `1000000`.
Base events keep policy	This drop-down list lets you select base events that you want to put in the correlation event: • **first**—this option is used to store the first base event of the event collection that triggered creation of the correlation event. This value is selected by default. • **last**—this option is used to store the last base event of the event collection that triggered creation of the correlation event. • **all**—this option is used to store all base events of the event collection that triggered creation of the correlation event.
Severity	Base coefficient used to determine the importance of a correlation rule: • **Critical** • **High** • **Medium** • **Low** (default)

Setting	Description
Order by	Event field to be used by selectors of the correlation rule to track the evolution of the situation. This can be useful, for example, if you want to configure a correlation rule to be triggered when several types of events occur in a sequence.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.
MITRE techniques	Downloaded MITRE ATT&CK techniques for analyzing the security coverage status using the MITRE ATT&CK matrix.
Use Unique fields mapping	This toggle switch allows you to save the values of unique fields to an array and pass it to a correlation event field. If the toggle switch is enabled, in the lower part of the **General** tab, an additional **Unique fields mapping** group of settings is displayed, in which you can configure the mapping of the source original unique fields to correlation event fields. When processing an event using a correlation rule, field mapping takes place first, and then operations from the **Actions** tab are applied to the correlation event resulting from the initial mapping. The toggle switch is turned off by default. Optional setting.

Unique field mapping group of settings

If you need to pass values of fields listed under **Unique fields** to the correlation event, here you can configure the mapping of unique fields to correlation event fields. This group of settings is displayed on the **General** tab if the **Use Unique fields mapping** toggle switch is enabled. Values of unique fields are an array, therefore the field in the correlation event must have the appropriate type: SA, NA, FA.

You can add a mapping by clicking the **Add** button and selecting a field from the drop-down list in the **Source event field** column. You can select fields specified in the **Unique fields** parameter. In the drop-down list in the **Destination event field** column, select the correlation event field to which you want to write the array of values of the source field. You can select fields whose type matches the type of the array (SA, NA, or FA, depending on the type of the source field).

You can delete one or more mappings by selecting the check boxes next to the relevant mappings and clicking **Delete**.

Selectors tab

This tab is used to define the conditions that the processed events must fulfill to trigger the correlation rule. To add a selector, click the **+ Add selector** button. You can add multiple selectors, reorder selectors, or remove selectors. To reorder selectors, use the reorder ⠿ icons. To remove a selector, click the delete ✕ icon next to it.

Each selector has a **Settings** tab and a **Local variables** tab.

The settings available on the **Settings** tab are described in the table below.

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Selector threshold (event count)	The number of events that must be received for the selector to trigger. The default value is `1`. Required setting.

Setting	Description

Recovery	This toggle switch lets the correlation rule not trigger when the selector receives the number of events specified in the **Selector threshold (event count)** field. This toggle switch is turned off by default.
	Example of how a selector works with the Recovery toggle switch enabled
	The **Recovery** switch is used in selectors of correlation rules to reset the bucket and prevent a correlation event from being generated. Typically, recovery is used together with the **On timeout** action.
	
	The **standard** correlation rule is configured as follows:
	• **Window, sec** is set to `300 seconds`.
	• On the **Actions** tab, the **On timeout** trigger is configured with the **Output** check box selected.
	• Two selectors have been added to the correlation rule:
	  • **Virus detected** (in the example, the `{"Message": "virus detected"}` event) with the **Recovery** toggle switch disabled.
	  • **Virus deleted** (in the example, the `{"Message": "virus deleted"}` event) with the **Recovery** toggle switch enabled.
	When a `{"Message": "virus detected"}` event is received, the bucket is started and the following happens:
	• A `{"Message": "virus deleted"}` event is not received within 300 seconds. In this case, the bucket is closed and the trigger generates a correlation event.
	• Within 300 seconds, a `{"Message": "virus deleted"}` event is received, which matches a selector with the **Recovery** toggle switch enabled. In this case, the bucket is cleared and no correlation event is generated.

Setting	Description
Filter	The filter that defines criteria for identifying events that trigger the selector when received. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. If you are going to use the filter in other correlation rules, you need to save it as a separate resource. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`/`Command`+`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value.

Setting	Description

	• **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
	  • **stream** (required) is the Kaspersky CyberTrace threat category.
	  • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
	  • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⣿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.
	Filtering based on data from the Extra event field

Setting	Description

	Conditions for filters based on data from the `Extra` event field:
	• Condition—**If**.
	• Left operand—**event field**.
	• In this event field, you can specify one of the following values:
	  • `Extra` field.
	  • Value from the `Extra` field in the following format:
	  `Extra.< field name >`
	  For example, `Extra.app`.
	  You must specify the value manually.
	  • Value from the array written to the `Extra` field in the following format:
	  `Extra.< field name >.< array element >`
	  For example, `Extra.array.0`.
	  The values in the array are numbered starting from 0. You must specify the value manually. To work with a value in the `Extra` field at a depth of 3 and lower, you must use backticks ``, for example, `` `Extra.lev1.lev2.lev3` ``.
	• Operator – =.
	• Right operand—**constant**.
	• Value—the value by which you need to filter events.
	The order of conditions specified in the selector filter of the correlation rule is significant and affects system performance. We recommend putting the most unique condition in the first place in the selector filter.
	Consider two examples of selector filters that select successful authentication events in Microsoft Windows.
	Selector filter 1:
	Condition 1: `DeviceProduct = Microsoft Windows`.
	Condition 2: `DeviceEventClassID = 4624`.
	Selector filter 2:
	Condition 1: `DeviceEventClassID = 4624`.
	Condition 2: `DeviceProduct = Microsoft Windows`.
	The order of conditions specified in selector filter 2 is preferable because it places less load on the system.

On the **Local variables** tab, you can add variables that will be valid inside the correlation rule. To add a variable, click the **+ Add** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete** button.

In the selector of the correlation rule, you can use regular expressions conforming to the RE2 standard. Using regular expressions in correlation rules is computationally intensive compared to other operations. When designing correlation rules, we recommend limiting the use of regular expressions to the necessary minimum and using other available operations.

To use a regular expression, you must use the `match` operator. The regular expression must be placed in a constant. The use of capture groups in regular expressions is optional. For the correlation rule to trigger, the field text matched against the regexp must exactly match the regular expression.

For a primer on the syntax and examples of correlation rules that use regular expressions in their selectors, refer to the following rules that are provided with KUMA:

- R105_04_Suspicious PowerShell commands. Suspected obfuscation.
- R333_Suspicious creation of files in the autorun folder.

Actions tab

You can use this tab to configure the triggers of the correlation rule. You can configure triggers on the following tabs:

- **On first threshold** triggers when the Bucket registers the first triggering of the selector during the lifetime of the Bucket.
- **On subsequent thresholds** triggers when the Bucket registers the second and all subsequent triggering of the selector during the lifetime of the Bucket.
- **On every threshold** triggers every time the Bucket registers the triggering of the selector.
- **On timeout** triggers when the lifetime of the Bucket ends, and is used together with a selector that has the **Recovery** check box selected in its settings. Thus, this trigger activates if the situation detected by the correlation rule is not resolved within the specified lifetime.

Available trigger settings are listed in the table below.

Setting	Description

Enrichment	Enrichment rules for modifying the values of correlation event fields. Enrichment rules are stored in the correlation rule where they were created. To create an enrichment rule, click the **+ Add enrichment** button. Available enrichment rule settings: • **Original type** is the type of the enrichment. When you select some enrichment types, additional settings may become available that you must specify. Available types of enrichment: • **constant** This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "constant" **Setting** / **Description** **Constant** — The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed. **Target field** — The event field to insert the data into. If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field. If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array. • **dictionary** This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "dictionary" **Setting** / **Description** **Dictionary name** — The dictionary from which the values are to be taken. **Key fields** — Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields. If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format. **Example**. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`. If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried. **Example**. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`. • **table** This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "table" **Setting** / **Description** **Dictionary name** — The dictionary from which the values are to be taken. **Key fields** — Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields. **Mapping** — Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`). The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field. If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

- **event**

  This type of enrichment is used when you need to write a value from another event field to the current event field. Available enrichment type settings are listed in the table below.

  Available enrichment type settings

Setting	Description
Target field	The KUMA event field that you want to populate with the data.
Source field	The event field whose value is written to the target field.

If you want to create a rule for modifying the raw data before writing to KUMA event fields, under **Conversion**, click the **+ Add conversion** button. In the **Type** drop-down list, select a conversion type. You can add multiple conversion by clicking the **+ Add conversion** button. To delete an added conversion, click the trashcan icon next to it.

Available conversions

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.
- **lower**—is used to make all characters of the value lowercase
- **upper**—is used to make all characters of the value uppercase
- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.
- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.
- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:
  - **Replace chars** specifies the sequence of characters to be replaced.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.
- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.
- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.
- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.
- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:
  - **Expression** is the RE2 regular expression whose results you want to replace.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.
- Converting encoded strings to text:
  - **decodeHexString**—used to convert a HEX string to text.
  - **decodeBase64String**—used to convert a Base64 string to text.
  - **decodeBase64URLString**—used to convert a Base64url string to text.
  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.
- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

When using enrichment of events that have **event**selected as the **Source kind** and the extended event schema fields are used as arguments, the following special considerations apply:

- If the source extended event schema field has the `Array of strings` type, and the target extended event schema field has the `String` type, the values are written to the target extended event schema field in TSV format.

  Example: the `SA.StringArray` extended event schema field contains values: `"string1"`, `"string2"`, `"string3"`. An event enrichment operation is performed. The result of the event enrichment operation is written to the `DeviceCustomString1` extended event schema field. The `DeviceCustomString1` extended event schema field contains values: `["string1", "string2", "string3"]`.

- If the source and target extended event schema fields have the `Array of strings` type, values of the source extended event schema field are added to the values of the target extended event schema field, and the `","` character is used as the delimiter.

  Example: The `SA.StringArrayOne` field of the extended event scheme contains the `["string1", "string2", "string3"]` values, and the `SA.StringArrayTwo` field of the extended event scheme contains the `["string4", "string5", "string6"]` values. An event enrichment operation is performed. The result of the event enrichment operation is written to the `SA.StringArrayTwo` field of the extended event scheme. The `SA.StringArrayTwo` extended event schema field contains values: `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **template**

  This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

  Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

  If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString .SA.StringArray}}
```

Required setting.

- The **Debug** toggle switch enables resource logging. This toggle switch is turned off by default.
- **Tags**

You can create multiple enrichment rules, reorder enrichment rules, or delete enrichment rules. To reorder enrichment rules, use the reorder ⣿ icons. To delete an enrichment rule, click the delete ✕ icon next to it.

Output	This check box enables the sending of correlation events for *post-processing*, that is, for external enrichment outside the correlation rule, for response, and to destinations. By default, this check box is cleared.
Loop to correlator	This check box enables the processing of the created correlation event by the rule chain of the current correlator. This makes hierarchical correlation possible. By default, this check box is cleared. If the **Output** and **Loop to correlator** check boxes are selected, the correlation rule is sent to post-processing first, and then to the selectors of the current correlation rule.
No alert	The check box disables the creation of alerts when the correlation rule is triggered. By default, this check box is cleared. If you do not want to create an alert when a correlation rule is triggered, but you still want to send a correlation event to the storage, select the **Output** and **No alert** check boxes. If you select only the **No alert** check box, a correlation event is not saved in the storage.

Categorization	Categorization rules for assets involved in the event. Using categorization rules, you can link and unlink only reactive categories to and from assets. To create an enrichment rule, click the **+ Add categorization** button.
	Available categorization rule settings:
	• **Action** is the operation applied to the category:
	  • **Add**: Link the category to the asset.
	  • **Delete**: Unlink the category from the asset.
	  Required setting.
	• **Event field** is the field of the event that contains the asset to which the operation will be applied.
	  Required setting.
	• **Category ID** is the category to which the operation will be applied.
	  Required setting.
	You can create multiple categorization rules, reorder categorization rules, or delete categorization rules. To reorder categorization rules, use the reorder ⣿ icons. To delete a categorization rule, click the delete ✕ icon next to it.

Active lists update	Operations with active lists. To create an operation with an active list, click the **+ Add active list action** button.
	Available parameters of an active list operation:
	• **Name** specifies the active list to which the operation is applied. If you want to edit the settings of an active list, click the pencil icon next to it.
	  Required setting.
	• **Operation** is the operation that is applied to the active list:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.
	  • **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Get**—get the Active list entry and write the values of the selected fields into the correlation event.
	  • **Delete**—delete the Active list entry.
	  Required setting.
	• **Key fields** are event fields that are used to create an active list entry. The specified event fields are also used as the key of the active list entry.
	  The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.
	  Required setting.
	• **Mapping**: Rules for mapping active list fields to event fields. You can use mapping rules if in the **Operation** drop-down list, you selected **Get** or **Set**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Active list field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.
	  • **KUMA field** is the event field to which the active list field is mapped.
	  • **Constant** is a constant that is assigned to the active list field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder ⣿ icons. To delete an operation with an active list, click the delete ✕ icon next to it.

Context tables update	Operations with context tables. To create an operation with a context table, click the **+ Add context table action** button.
	Available parameters of a context table operation:
	• **Name** specifies the context table to which the operation is applied. If you want to edit the settings of a context table, click the pencil icon next to it.
	Required setting.
	• **Operation** is the operation that is applied to the context table:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table. This operation is used only for fields of `Number` and `Float` types.
	  • **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
	  • **Get**—get the fields of the context table and write the values of the specified fields into the correlation event. Table fields of the boolean type and lists of boolean values are excluded from mapping because the event does not contain boolean fields.
	  • **Delete**—delete the context table entry.
	  Required setting.
	• **Mapping**: Rules for mapping context table fields to event fields or variables. You can use mapping rules if in the **Operation** drop-down list, you selected something other than **Delete**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Context table field** is the context table field that is mapped to an event field. You cannot specify a context table field that is already used in a mapping. You can specify tabulation characters, special characters, or just numbers. The maximum length of a context table field name is 128 characters. A context table field name cannot begin with an underscore.
	  • **KUMA field** is the event field or local variable to which the context table field is mapped.
	  • **Constant** is a constant that is assigned to the context table field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**, **Merge**, or **Sum**. The maximum length of a constant is 1024 characters.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with context tables, reorder operations with context tables, or delete operations with context tables. To reorder operations with context tables, use the reorder icons. To delete an operation with a context tables, click the delete icon next to it.

Correlators tab

This tab is displayed only when you edit the settings of the created correlation rule; on this tab, you can link the correlation rule to a correlator.

To link the correlation rule to a correlator, click **Link to service** → **Link to correlator** button, in the displayed window, specify one or more correlators, and click the **OK** button. The correlation rule is linked to the specified correlators and added to the end of the execution queue in the correlator settings. If you want to change the position of a correlation rule in the execution queue, go to the **Resources** → **Correlator** section, click the correlator, and in the displayed window, go to the **Correlation** section, select the check box next to the correlation rule, and change the position of the correlation rule by clicking the **Move up** and **Move down** buttons.

You can add multiple correlators or delete correlators. To do this, select the check box next to the correlator, click the **Delete** button, and confirm deletion.

Correlation rules of the 'simple' type

Correlation rules of the **simple** type are used to define simple sequences of events. Settings for a correlation rule of the **simple** type are described in the following tables.

In comparison with the data model of the normalized event, some fields of the correlation event formed by the **simple** correlation rule may be different (see the table below).

Name of the correlation event field	Description
StartTime	Creation date and time (timestamp) of the base event from which the correlation event was generated.
EndTime	Creation date and time (timestamp) of the base event from which the correlation event was generated.

General tab

This tab lets you specify the general settings of the correlation rule.

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Correlation rule type: **simple**. Required setting.
Tags	Tags for resource search. Optional setting.
Propagated fields	Event fields by which events are selected. If a selector specified on the **Selectors** tab is triggered, the selected event fields are copied to the correlation event.
Rate limit	Maximum number of times a correlation rule can be triggered per second. The default value is `0`. If correlation rules employing complex logic for pattern detection are not triggered, this may be due to the way rule triggers are counted in KUMA. In this case, we recommend increasing the **Rate limit**, for example, to `1000000`.
Severity	Base coefficient used to determine the importance of a correlation rule: • **Critical** • **High** • **Medium** • **Low** (default)
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.
MITRE techniques	Downloaded MITRE ATT&CK techniques for analyzing the security coverage status using the MITRE ATT&CK matrix.

Selectors tab

This tab is used to define the conditions that the processed events must fulfill to trigger the correlation rule. A selector has a **Settings** tab and a **Local variables** tab.

The settings available on the **Settings** tab are described in the table below.

Setting	Description
Filter	The filter that defines criteria for identifying events that trigger the selector when received. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. If you are going to use the filter in other correlation rules, you need to save it as a separate resource. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **Ctrl**/**Command**+**F1**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.
	Filtering based on data from the Extra event field
	Conditions for filters based on data from the `Extra` event field:
	• Condition—**If**.
	• Left operand—**event field**.

Setting	Description

	• In this event field, you can specify one of the following values:
	  • `Extra` field.
	  • Value from the `Extra` field in the following format:
	  `Extra.< field name >`
	  For example, `Extra.app`.
	  You must specify the value manually.
	  • Value from the array written to the `Extra` field in the following format:
	  `Extra.< field name >.< array element >`
	  For example, `Extra.array.0`.
	  The values in the array are numbered starting from 0. You must specify the value manually. To work with a value in the `Extra` field at a depth of 3 and lower, you must use backticks ``, for example, `` `Extra.lev1.lev2.lev3` ``.
	• Operator – =.
	• Right operand—**constant**.
	• Value—the value by which you need to filter events.
	The order of conditions specified in the selector filter of the correlation rule is significant and affects system performance. We recommend putting the most unique condition in the first place in the selector filter.
	Consider two examples of selector filters that select successful authentication events in Microsoft Windows.
	Selector filter 1:
	Condition 1: `DeviceProduct = Microsoft Windows`.
	Condition 2: `DeviceEventClassID = 4624`.
	Selector filter 2:
	Condition 1: `DeviceEventClassID = 4624`.
	Condition 2: `DeviceProduct = Microsoft Windows`.
	The order of conditions specified in selector filter 2 is preferable because it places less load on the system.

On the **Local variables** tab, you can add variables that will be valid inside the correlation rule. To add a variable, click the **+ Add** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete** button.

Actions tab

You can use this tab to configure the trigger of the correlation rule. A correlation rule of the **simple** type can have only one trigger, which is activated each time the bucket registers the selector triggering. Available trigger settings are listed in the table below.

Setting	Description

Enrichment	Enrichment rules for modifying the values of correlation event fields. Enrichment rules are stored in the correlation rule where they were created. To create an enrichment rule, click the **+ Add enrichment** button. Available enrichment rule settings: • **Original type** is the type of the enrichment. When you select some enrichment types, additional settings may become available that you must specify. Available types of enrichment: • **constant** This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "constant" **Setting** / **Description** **Constant** — The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed. **Target field** — The event field to insert the data into. If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field. If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array. • **dictionary** This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "dictionary" **Setting** / **Description** **Dictionary name** — The dictionary from which the values are to be taken. **Key fields** — Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields. If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format. **Example**. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`. If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried. **Example**. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`. • **table** This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below. Parameters of enrichment type "table" **Setting** / **Description** **Dictionary name** — The dictionary from which the values are to be taken. **Key fields** — Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields. **Mapping** — Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`). The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field. If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

- **event**

  This type of enrichment is used when you need to write a value from another event field to the current event field. Available enrichment type settings are listed in the table below.

  Available enrichment type settings

Setting	Description
Target field	The KUMA event field that you want to populate with the data.
Source field	The event field whose value is written to the target field.

If you want to create a rule for modifying the raw data before writing to KUMA event fields, under **Conversion**, click the **+ Add conversion** button. In the **Type** drop-down list, select a conversion type. You can add multiple conversion by clicking the **+ Add conversion** button. To delete an added conversion, click the trashcan icon next to it.

Available conversions

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.
- **lower**—is used to make all characters of the value lowercase
- **upper**—is used to make all characters of the value uppercase
- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.
- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.
- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:
  - **Replace chars** specifies the sequence of characters to be replaced.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.
- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.
- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.
- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.
- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:
  - **Expression** is the RE2 regular expression whose results you want to replace.
  - **With chars** is the character sequence to be used instead of the character sequence being replaced.
- Converting encoded strings to text:
  - **decodeHexString**—used to convert a HEX string to text.
  - **decodeBase64String**—used to convert a Base64 string to text.
  - **decodeBase64URLString**—used to convert a Base64url string to text.
  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

  During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

  If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

  We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.
- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.

- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

When using enrichment of events that have **event**selected as the **Source kind** and the extended event schema fields are used as arguments, the following special considerations apply:

- If the source extended event schema field has the `Array of strings` type, and the target extended event schema field has the `String` type, the values are written to the target extended event schema field in TSV format.

  Example: the `SA.StringArray` extended event schema field contains values: `"string1"`, `"string2"`, `"string3"`. An event enrichment operation is performed. The result of the event enrichment operation is written to the `DeviceCustomString1` extended event schema field. The `DeviceCustomString1` extended event schema field contains values: `["string1", "string2", "string3"]`.

- If the source and target extended event schema fields have the `Array of strings` type, values of the source extended event schema field are added to the values of the target extended event schema field, and the `","` character is used as the delimiter.

  Example: The `SA.StringArrayOne` field of the extended event scheme contains the `["string1", "string2", "string3"]` values, and the `SA.StringArrayTwo` field of the extended event scheme contains the `["string4", "string5", "string6"]` values. An event enrichment operation is performed. The result of the event enrichment operation is written to the `SA.StringArrayTwo` field of the extended event scheme. The `SA.StringArrayTwo` extended event schema field contains values: `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **template**

  This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

  Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

  If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

  - `{{.SA.StringArrayOne}}`
  - `{{- range $index, $element := . SA.StringArrayOne -}}`
    `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

  To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString .SA.StringArray}}
```

Required setting.

- The **Debug** toggle switch enables resource logging. This toggle switch is turned off by default.
- **Tags**

You can create multiple enrichment rules, reorder enrichment rules, or delete enrichment rules. To reorder enrichment rules, use the reorder ⣿ icons. To delete an enrichment rule, click the delete ✕ icon next to it.

Output	This check box enables the sending of correlation events for *post-processing*, that is, for external enrichment outside the correlation rule, for response, and to destinations. By default, this check box is cleared.
Loop to correlator	This check box enables the processing of the created correlation event by the rule chain of the current correlator. This makes hierarchical correlation possible. By default, this check box is cleared. If the **Output** and **Loop to correlator** check boxes are selected, the correlation rule is sent to post-processing first, and then to the selectors of the current correlation rule.
No alert	The check box disables the creation of alerts when the correlation rule is triggered. By default, this check box is cleared. If you do not want to create an alert when a correlation rule is triggered, but you still want to send a correlation event to the storage, select the **Output** and **No alert** check boxes. If you select only the **No alert** check box, a correlation event is not saved in the storage.

Categorization	Categorization rules for assets involved in the event. Using categorization rules, you can link and unlink only reactive categories to and from assets. To create an enrichment rule, click the **+ Add categorization** button.
	Available categorization rule settings:
	• **Action** is the operation applied to the category:
	  • **Add**: Link the category to the asset.
	  • **Delete**: Unlink the category from the asset.
	  Required setting.
	• **Event field** is the field of the event that contains the asset to which the operation will be applied.
	  Required setting.
	• **Category ID** is the category to which the operation will be applied.
	  Required setting.
	You can create multiple categorization rules, reorder categorization rules, or delete categorization rules. To reorder categorization rules, use the reorder ⣿ icons. To delete a categorization rule, click the delete ✕ icon next to it.

Active lists update	Operations with active lists. To create an operation with an active list, click the **+ Add active list action** button.
	Available parameters of an active list operation:
	• **Name** specifies the active list to which the operation is applied. If you want to edit the settings of an active list, click the pencil icon next to it.
	  Required setting.
	• **Operation** is the operation that is applied to the active list:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.
	  • **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Get**—get the Active list entry and write the values of the selected fields into the correlation event.
	  • **Delete**—delete the Active list entry.
	  Required setting.
	• **Key fields** are event fields that are used to create an active list entry. The specified event fields are also used as the key of the active list entry.
	  The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.
	  Required setting.
	• **Mapping**: Rules for mapping active list fields to event fields. You can use mapping rules if in the **Operation** drop-down list, you selected **Get** or **Set**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Active list field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.
	  • **KUMA field** is the event field to which the active list field is mapped.
	  • **Constant** is a constant that is assigned to the active list field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder ⣿ icons. To delete an operation with an active list, click the delete ✕ icon next to it.

Context tables update	Operations with context tables. To create an operation with a context table, click the **+ Add context table action** button.
	Available parameters of a context table operation:
	• **Name** specifies the context table to which the operation is applied. If you want to edit the settings of a context table, click the pencil icon next to it.
	Required setting.
	• **Operation** is the operation that is applied to the context table:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table. This operation is used only for fields of `Number` and `Float` types.
	  • **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
	  • **Get**—get the fields of the context table and write the values of the specified fields into the correlation event. Table fields of the boolean type and lists of boolean values are excluded from mapping because the event does not contain boolean fields.
	  • **Delete**—delete the context table entry.
	  Required setting.
	• **Mapping**: Rules for mapping context table fields to event fields or variables. You can use mapping rules if in the **Operation** drop-down list, you selected something other than **Delete**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Context table field** is the context table field that is mapped to an event field. You cannot specify a context table field that is already used in a mapping. You can specify tabulation characters, special characters, or just numbers. The maximum length of a context table field name is 128 characters. A context table field name cannot begin with an underscore.
	  • **KUMA field** is the event field or local variable to which the context table field is mapped.
	  • **Constant** is a constant that is assigned to the context table field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**, **Merge**, or **Sum**. The maximum length of a constant is 1024 characters.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with context tables, reorder operations with context tables, or delete operations with context tables. To reorder operations with context tables, use the reorder icons. To delete an operation with a context tables, click the delete icon next to it.

Correlators tab

This tab is displayed only when you edit the settings of the created correlation rule; on this tab, you can link the correlation rule to a correlator.

To link the correlation rule to a correlator, click **Link to service** → **Link to correlator** button, in the displayed window, specify one or more correlators, and click the **OK** button. The correlation rule is linked to the specified correlators and added to the end of the execution queue in the correlator settings. If you want to change the position of a correlation rule in the execution queue, go to the **Resources** → **Correlator** section, click the correlator, and in the displayed window, go to the **Correlation** section, select the check box next to the correlation rule, and change the position of the correlation rule by clicking the **Move up** and **Move down** buttons.

You can add multiple correlators or delete correlators. To do this, select the check box next to the correlator, click the **Delete** button, and confirm deletion.

Correlation rules of the 'operational' type

Correlation rules of the **operational** type are used for working with active lists. Settings for a correlation rule of the **operational** type are described in the following tables.

General tab

This tab lets you specify the general settings of the correlation rule.

Setting	Description
Name	Unique name of the resource. The maximum length of the name is 128 Unicode characters. Required setting.
Tenant	The name of the tenant that owns the resource. Required setting.
Type	Correlation rule type: **operational**. Required setting.
Tags	Tags for resource search. Optional setting.
Rate limit	Maximum number of times a correlation rule can be triggered per second. The default value is `0`. If correlation rules employing complex logic for pattern detection are not triggered, this may be due to the way rule triggers are counted in KUMA. In this case, we recommend increasing the **Rate limit**, for example, to `1000000`.
Description	Description of the resource. The maximum length of the description is 4000 Unicode characters.
MITRE techniques	Downloaded MITRE ATT&CK techniques for analyzing the security coverage status using the MITRE ATT&CK matrix.

Selectors tab

This tab is used to define the conditions that the processed events must fulfill to trigger the correlation rule. A selector has a **Settings** tab and a **Local variables** tab.

The settings available on the **Settings** tab are described in the table below.

Setting	Description
Filter	The filter that defines criteria for identifying events that trigger the selector when received. You can select an existing filter or create a new filter. To create a new filter, select **Create new**. If you want to edit the settings of an existing filter, click the pencil icon next to it. If you are going to use the filter in other correlation rules, you need to save it as a separate resource. **How to create a filter?** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.
	Filtering based on data from the Extra event field
	Conditions for filters based on data from the `Extra` event field:
	• Condition—**If**.
	• Left operand—**event field**.

Setting	Description

	• In this event field, you can specify one of the following values:
	  • `Extra` field.
	  • Value from the `Extra` field in the following format:
	  `Extra.< field name >`
	  For example, `Extra.app`.
	  You must specify the value manually.
	  • Value from the array written to the `Extra` field in the following format:
	  `Extra.< field name >.< array element >`
	  For example, `Extra.array.0`.
	  The values in the array are numbered starting from 0. You must specify the value manually. To work with a value in the `Extra` field at a depth of 3 and lower, you must use backticks ``, for example, `` `Extra.lev1.lev2.lev3` ``.
	• Operator – =.
	• Right operand—**constant**.
	• Value—the value by which you need to filter events.
	The order of conditions specified in the selector filter of the correlation rule is significant and affects system performance. We recommend putting the most unique condition in the first place in the selector filter.
	Consider two examples of selector filters that select successful authentication events in Microsoft Windows.
	Selector filter 1:
	Condition 1: `DeviceProduct = Microsoft Windows`.
	Condition 2: `DeviceEventClassID = 4624`.
	Selector filter 2:
	Condition 1: `DeviceEventClassID = 4624`.
	Condition 2: `DeviceProduct = Microsoft Windows`.
	The order of conditions specified in selector filter 2 is preferable because it places less load on the system.

On the **Local variables** tab, you can add variables that will be valid inside the correlation rule. To add a variable, click the **+ Add** button, then specify the variable and its value. You can add multiple variables or delete variables. To delete a variable, select the check box next to it and click the **Delete** button.

Actions tab

You can use this tab to configure the trigger of the correlation rule. A correlation rule of the **operational** type can have only one trigger, which is activated each time the bucket registers the selector triggering. Available trigger settings are listed in the table below.

Setting	Description

Active lists update	Operations with active lists. To create an operation with an active list, click the **+ Add active list action** button.
	Available parameters of an active list operation:
	• **Name** specifies the active list to which the operation is applied. If you want to edit the settings of an active list, click the pencil icon next to it.
	Required setting.
	• **Operation** is the operation that is applied to the active list:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the active list.
	  • **Set**—write the values of the selected fields of the correlation event into the Active list by creating a new or updating an existing Active list entry. When the Active list entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Get**—get the Active list entry and write the values of the selected fields into the correlation event.
	  • **Delete**—delete the Active list entry.
	  Required setting.
	• **Key fields** are event fields that are used to create an active list entry. The specified event fields are also used as the key of the active list entry.
	  The active list entry key depends on the available event fields and does not depend on the order in which they are displayed in the KUMA web interface.
	  Required setting.
	• **Mapping**: Rules for mapping active list fields to event fields. You can use mapping rules if in the **Operation** drop-down list, you selected **Get** or **Set**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Active list field** is the active list field that is mapped to the event field. The field must not contain special characters or numbers only.
	  • **KUMA field** is the event field to which the active list field is mapped.
	  • **Constant** is a constant that is assigned to the active list field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with active lists, reorder operations with active lists, or delete operations with active lists. To reorder operations with active lists, use the reorder icons. To delete an operation with an active list, click the delete icon next to it.

Setting	Description

Context tables update	Operations with context tables. To create an operation with a context table, click the **+ Add context table action** button.
	Available parameters of a context table operation:
	• **Name** specifies the context table to which the operation is applied. If you want to edit the settings of a context table, click the pencil icon next to it.
	Required setting.
	• **Operation** is the operation that is applied to the context table:
	  • **Sum**—add a constant, the value of a correlation event field, or the value of a local variable to the value of the context table. This operation is used only for fields of `Number` and `Float` types.
	  • **Set**—write the values of the selected fields of the correlation event into the context table by creating a new or updating an existing context table entry. When the context table entry is updated, the data is merged and only the specified fields are overwritten.
	  • **Merge**—append the value of a correlation event field, local variable, or constant to the current value of a field of the context table.
	  • **Get**—get the fields of the context table and write the values of the specified fields into the correlation event. Table fields of the boolean type and lists of boolean values are excluded from mapping because the event does not contain boolean fields.
	  • **Delete**—delete the context table entry.
	  Required setting.
	• **Mapping**: Rules for mapping context table fields to event fields or variables. You can use mapping rules if in the **Operation** drop-down list, you selected something other than **Delete**. To create a mapping rule, click the **+ Add** button.
	  Available mapping rule settings:
	  • **Context table field** is the context table field that is mapped to an event field. You cannot specify a context table field that is already used in a mapping. You can specify tabulation characters, special characters, or just numbers. The maximum length of a context table field name is 128 characters. A context table field name cannot begin with an underscore.
	  • **KUMA field** is the event field or local variable to which the context table field is mapped.
	  • **Constant** is a constant that is assigned to the context table field. You need to specify a constant if in the **Operation** drop-down list, you selected **Set**, **Merge**, or **Sum**. The maximum length of a constant is 1024 characters.
	  You can create multiple mapping rules or delete mapping rules. To delete a mapping rule, select the check box next to it and click **Delete**.
	You can create multiple operations with context tables, reorder operations with context tables, or delete operations with context tables. To reorder operations with context tables, use the reorder icons. To delete an operation with a context tables, click the delete icon next to it.

Correlators tab

This tab is displayed only when you edit the settings of the created correlation rule; on this tab, you can link the correlation rule to a correlator.

To link the correlation rule to a correlator, click **Link to service** → **Link to correlator** button, in the displayed window, specify one or more correlators, and click the **OK** button. The correlation rule is linked to the specified correlators and added to the end of the execution queue in the correlator settings. If you want to change the position of a correlation rule in the execution queue, go to the **Resources** → **Correlator** section, click the correlator, and in the displayed window, go to the **Correlation** section, select the check box next to the correlation rule, and change the position of the correlation rule by clicking the **Move up** and **Move down** buttons.

You can add multiple correlators or delete correlators. To do this, select the check box next to the correlator, click the **Delete** button, and confirm deletion.

Using filters in correlation rules

As the number of correlation rules increases, their maintenance becomes more complex. You may need to modify filter settings for several correlation rules at once. For example, you can add exclusions to improve detection accuracy or modify filter conditions when normalization settings change or when expanding rule coverage.

If you modify the filter settings of each correlation rule individually and do not save the filter as a named resource, the risk of introducing errors in the filter increases over time. As a result, different filter settings may be specified in similar correlation rules, since one of the rules was updated and the other was not. This approach also makes it harder to read filter conditions because the same condition in different rules can be specified in different ways, or several conditions can be specified in a different order.

To solve this problem, it is recommended to use filters as named resources that can be reused across different correlation rules. In this case, to apply new filter settings, you only need to modify the filter itself, and the updated settings will be automatically applied to all correlation rules in which this filter is specified.

How to save a filter as a resource

To create a filter as a named resource,

do one of the following:

- Create a filter in the **Resources** section.
- In the window for creating or editing a resource, when configuring a filter, select the **Save filter** check box, then specify a name for the new filter. For example, when creating or editing a correlation rule, the filter is configured on the **Selectors** tab.

The filter is created and added to the filter list.

Examples

Examples of using filters in correlation rules:

- There are correlation rules that specify the same type of events in their trigger conditions, for example, `DeviceEventClassID='4688'` (process start).

  You can create a filter, specify this condition in it, and save it under an appropriate name, for example, `4688: A new process has been created`. This filter can then be used in all rules that are triggered based on this event type.

- You need to exclude legitimate events from correlation logic, such as administrator actions. All administrator account names start with `adm_`.

  You can create a filter, specify such a condition in it, and save it under an appropriate name, for example, `Exclusions: adm_`. You can save each of the exclusion conditions as a separate filter with the `Exclusions:` prefix in the name. As a result, you get a set of filters for exclusions. This approach makes it easier to maintain rules and analyze exclusions.

Examples of commonly used filters:

- Filters for types of event sources (for example, Windows, Linux).
- Filters to apply rules only to specific hosts (for example, a domain controller host) or accounts (for example, service accounts or users from a specific department).
- Filters for commonly used exclusions.

- Filters for specific types of KUMA events (for example, base events or correlation events).
- Filters for specific events (for example, Windows interactive authentication types).

Limiting how many times a correlation rule can be triggered

If a correlation rule is to be triggered a limited number of times within a certain period, this number can be stored in an active list and used when processing the rule. Suppose you need to limit the number of times the correlation rule is triggered to ten per day. For this purpose, a trigger counter is stored in the active list, and a separate entry is used for each rule and for each date. When a rule is triggered, the counter is incremented by one, and after reaching 10, the rule should not be triggered again until the beginning of the next day.

Configuring a trigger limit for a correlation rule involves the following steps:

1 Create an active list

Create an active list that will store the number of times the correlation rule has been triggered.

1. In the web interface, go to the **Resources** → **Active lists** section.
2. Then click the **Create** button.
3. Manage the settings of the active list:
   a. In the **Name** field, specify a name such as `correlation_limits`.
   b. In the **Tenant** drop-down list, select a tenant.
   c. In the **Time to live** field, enter the storage duration for the active list entry.
4. If necessary, fill in the **Tags** and **Description** fields.
5. Click the **Save** button.

The active list is added.

As the field for storing the trigger count, use `_count`. To write the active list, specify a key made up of the name of the correlation rule and the date of the event (for example, `LimitRule_Example_2026-09-06`). Such a key allows storing a separate counter for each correlation rule and for each day.

2 Configure a correlation rule

1. Create or open the settings for an existing correlation rule of the **standard** type.
2. On the **General** tab, specify the basic settings of the rule, including **Name**, **Tenant**, and **Kind**.
3. On the **Selectors** tab, configure the conditions that the rule applies to select events.

4. Select the **Actions** tab.

5. Under **Active lists update**, click the **+ Add active list action** button and manage the following settings:

   a. In the **Name** field, select the previously created active list.

   b. In the **Operation** field, select an operation with the counter:

   - **Get** to get the current value of `_count`.
   - **Install** to create or update an entry.
   - **Add** to increment the counter.

6. Use **Key fields** to for access to an individual entry in the active list. Key fields must include the event fields that make up the entry key: the name of the correlation rule and the date of the event.

7. Under **Mapping**, configure the mapping between the `_count` field and the event field, if necessary for the selected operation.

8. Configure the processing of the resulting `_count` value:

   - If there is no entry for the current date, the counter must be set to 1.
   - If the `_count` is less than 10, the counter must be incremented by 1, and the rule must be triggered.
   - If `_count` is 10, the rule should not trigger.

9. Save the correlation rule.

❸ Linking the active list to a correlation rule

Link the active list to a correlation rule, and the correlation rule to a correlator.

1. Open the created correlation rule.

2. Select the **Services** tab.

3. Click **Link to service** → **Link to correlator**.

4. This opens a window; in that window, select one or more correlators.

5. Click **OK**.

After linkig, the correlation rule is added to the execution queue of the selected correlator. If necessary, you can change its position in the queue in the **Resources** → **Correlators** → **[the relevant correlator]** → **Correlation** section using the **Move up** and **Move down** buttons.

Make sure that the active list is available for the correlator to which the correlation rule is linked.

4 Verifying the result

Send some sample events that match the conditions of the correlation rule's selector to check the number of hits and the `_count` value in the active list.

1. Send the first event.

   Make sure that the rule has been triggered and an entry has been created in the active list for the current date with `_count = 1`.

2. Send eight more events one by one.

   Verify that the rule continues to trigger and that the `_count` value has increased to 9.

3. Send the tenth event.

   Make sure that the rule is triggered and the `_count` is 10.

4. Send another event that matches the conditions of the selector.

   Make sure that the rule has not been triggered and that the `_count` remains at 10.

5. When the next day comes, send an event that matches the selector conditions.

   Verify that a new active list entry is being used for the new date, and the rule can be triggered again.

To view the entries in an active list, go to **Resources** → **Active lists** and select an active list. This opens a table with the **Key**, **Value**, **Expiration date**, **Updated** , and other parameters of the entry.

Variables in correlators

If tracking values in event fields, active lists, or dictionaries is not enough to cover some specific security scenarios, you can use global and local *variables*. You can use them to take various actions on the values received by the correlators by implementing complex logic for threat detection. Variables can be declared in the correlator (*global variables*) or in the correlation rule (*local variables*) by assigning a function to them, then querying them from correlation rules as if they were ordinary event fields and receiving the triggered function result in response.

Usage scope of variables:

- When searching for identical or unique field values in correlation rules.
- In the correlation rule selectors, in the filters of the conditions under which the correlation rule must be triggered.
- When enriching correlation events. Select **Event** as the source type.
- When populating active lists with values.

Variables can be queried the same way as event fields by preceding their names with the $ character.

You can use extended event schema fields in correlation rules, local variables, and global variables.

Local variables in identical and unique fields

You can use local variables in the **Identical fields** and **Unique fields** sections of 'standard' type correlation rules. To use a local variable, its name must be preceded with the "$" character.

For an example of using local variables in the **Identical fields** and **Unique fields** sections, refer to the rule provided with KUMA: R403_Access to malicious resources from a host with disabled protection or an out-of-date anti-virus database.

Local variables in selector

To use a local variable in a selector:

1. Add a local variable to the rule.
2. In the **Correlation rules** window, go to the **General** tab and add the created local variable to the **Identical fields** section. Prefix the local variable name with a "$" character.
3. In **Correlation rules** window, go to the **Selectors** tab, select an existing filter or create a new filter and click **Add condition**.
4. Select the **event field** as the operand.
5. Select the local variable as the event field value and prefix the variable name with a "$" character.
6. Specify the remaining filter settings.
7. Click **Save**.

For an example of using local variables, refer to the rule provided with KUMA: R403_Access to malicious resources from a host with disabled protection or an out-of-date anti-virus database.

Local Variables in event enrichment

You can use 'standard' and 'simple' correlation rules to enrich events with local variables.

Enrichment with text and numbers

You can enrich events with text (strings). To do so, you can use functions that modify strings: to_lower, to_upper, str_join, append, prepend, substring, tr, replace, str_join.

You can enrich events with numbers. To do so, you can use the following functions: addition ("+"), subtraction ("-"), multiplication ("*"), division ("/"), round, ceil, floor, abs, pow.

You can also use regular expressions to manage data in local variables.

Using regular expressions in correlation rules is computationally intensive compared to other operations. Therefore, when designing correlation rules, we recommend limiting the use of regular expressions to the necessary minimum and using other available operations.

Timestamp enrichment

You can enrich events with timestamps (date and time). To do so, you can use functions that let you get or modify timestamps: now, extract_from_timestamp, parse_timestamp, format_timestamp, truncate_timestamp, time_diff.

Operations with active lists and tables

You can enrich events with local variables and data from active lists and tables.

To enrich events with data from an active list, use the active_list, active_list_dyn functions.

To enrich events with data from a table, use the table_dict, dict functions.

You can create conditional statements by using the 'conditional' function in local variables. In this way, the variable can return one of the values depending on what data was received for processing.

Enriching events with a local variable

To use a local variable to enrich events:

1. Add a local variable to the rule.
2. In the **Correlation rules** window, go to the **General** tab and add the created local variable to the **Identical fields** section. Prefix the local variable name with a "$" character.
3. In the **Correlation rules** window, go to the **Actions** tab, and under **Enrichment**, in the **Source kind** drop-down list, select **event**.
4. From the **Target field** drop-down list, select the KUMA event field to which you want to pass the value of the local variable.
5. From the **Source field** drop-down list, select a local variable. Prefix the local variable name with a "$" character.
6. Specify the remaining rule settings.
7. Click **Save**.

Local variables in active list enrichment

You can use local variables to enrich active lists.

To enrich the active list with a local variable:

1. Add a local variable to the rule.
2. In the **Correlation rules** window, go to the **General** tab and add the created local variable to the **Identical fields** section. Prefix the local variable name with a "$" character.
3. In the **Correlation rules** window, go to the **Actions** tab and under **Active lists update**, add the local variable to the **Key fields** field. Prefix the local variable name with a "$" character.
4. Under **Mapping**, specify the correspondence between the event fields and the active list fields.
5. Click the **Save** button.

Properties of variables

Local and global variables

The properties of global variables differ from the properties of local variables.

Global variables:

- Global variables are declared at the correlator level and are applied only within the scope of this correlator.
- The global variables of the correlator can be queried from all correlation rules that are specified in it.
- In standard correlation rules, the same global variable can take different values in each selector.
- It is not possible to transfer global variables between different correlators.

Local variables:

- Local variables are declared at the correlation rule level and are applied only within the limits of this rule.
- In standard correlation rules, the scope of a local variable consists of only the selector in which the variable was declared.
- Local variables can be declared in any type of correlation rule.
- Local variables cannot be transferred between rules or selectors.
- A local variable cannot be used as a global variable.

Variables used in various types of correlation rules

- In **operational** correlation rules, on the **Actions** tab, you can specify all variables available or declared in this rule.
- In **standard** correlation rules, on the **Actions** tab, you can provide only those variables specified in these rules on the **General** tab, in the **Identical fields** field.
- In **simple** correlation rules, on the **Actions** tab, you can provide only those variables specified in these rules on the **General** tab, in the **Inherited Fields** field.

Requirements for variables

When adding a variable function, you must first specify the name of the function, and then list its parameters in parentheses. Basic mathematical operations (addition, subtraction, multiplication, division) are an exception to this requirement. When these operations are used, parentheses are used to designate the severity of the operations.

Requirements for function names:

- Must be unique within the correlator.
- Must contain 1 to 128 Unicode characters.

- Must not begin with the character $.
- Must be written in camelCase or CamelCase.

Special considerations when specifying functions of variables:

- The sequence of parameters is important.
- Parameters are separated by a comma: `,`.
- String parameters are passed in single quotes: `'`.
- Event field names and variables are specified without quotation marks.
- When querying a variable as a parameter, add the `$` character before its name.
- You do not need to add a space between parameters.
- In all functions in which a variable can be used as parameters, nested functions can be created.

Functions of variables

Operations with active lists and dictionaries

active_list and active_list_dyn

Gets data from an active list and dynamically generates an active list field name and a key.

You must specify the parameters in the following sequence:

1. Active list name.
2. Expression that returns the field name of the active list
3. One or more expressions whose results make up the key

Example

```
active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))
```

Result: field values of the active list are obtained.

You can use these functions to reference an active list of the Shared tenant from a variable. To do so, add the `@Shared` suffix after the name of the active list (case sensitive).

Example

```
active_list('exampleActiveList@Shared', 'score', SourceAddress, SourceUserName)
```

table_dict

Gets information about the value in the specified column of a dictionary of the `table` type.

You must specify the parameters in the following sequence:

1. Dictionary name
2. Dictionary column name
3. One or more expressions whose results make up the dictionary string key

```
Example
table_dict('exampleTableDict', 'office', SourceUserName)
```

Result: data is obtained from the `exampleTableDict` dictionary from the row with the `SourceUserName` key in the `office` column.

```
Example
table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))
```

Result: data is obtained from the `exampleTableDict` dictionary from a composite key string from the `SourceAddress` field value and the lowercase value of the `SourceUserName` field from the `office` column.

You can use this function to reference a dictionary of the Shared tenant from a variable. To do so, add the `@Shared` suffix after the name of the active list (case sensitive).

```
Example
table_dict('exampleTableDict@Shared', 'office', SourceUserName)
```

dict

Gets information about the value in the specified column of a dictionary of the `dictionary` type.

You must specify the parameters in the following sequence:

1. Dictionary name.
2. One or more expressions whose results are used to generate the dictionary row key.

```
Example
dict('exampleDictionary', SourceAddress)
```

Result: data is obtained from `exampleDictionary` from the row with the `SourceAddress` key.

```
Example
dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))
```

Result: data is obtained from the `exampleDictionary` dictionary from a composite key string from the `SourceAddress` field value and the lowercase value of the `SourceUserName` field.

You can use this function to reference a dictionary of the Shared tenant from a variable. To do so, add the `@Shared` suffix after the name of the active list (case sensitive).

```
Example

dict('exampleDictionary@Shared', SourceAddress)
```

Operations with context tables

context_table

Returns the value of the specified field from the context table.

You must specify the parameters in the following sequence:

1. Name of the context table. The name must be specified.
2. Name of the field whose value you want to get.
3. Name of the key field to be compared to.
4. Expression that returns the value for comparison with the value of the key field from item 3.

At least four parameters must be passed to the function.

```
Example

context_table('test_table', 'Username', 'IP', DestinationAddress)
```

Result: getting the value of the specified field from a row of the context table for which the key field matches the value passed in the comparison parameter. If the table is missing, or there are no matches, or the field is not found, an empty string is returned.

You can use this function to reference a context table of the Shared tenant from a variable. To do so, add the `@Shared` suffix after the name of the context table (case sensitive).

```
Example

context_table('test_table@Shared', SourceAddress)
```

len

Returns the length of a string or array.

The function returns the length of the array if the passed array belongs to one of the following types:

- array of integers
- array of floats
- array of strings
- array of booleans

If an array of a different type is passed, the data of the array is cast to the string type, and the function returns the length of the resulting string.

Example

```
len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))
```

Example

```
len(DeviceCustomString1)
```

distinct_items

Returns a list of unique elements in an array.

The function returns the list of unique array elements if the passed array belongs to one of the following types:

- array of integers
- array of floats
- array of strings
- array of booleans

If an array of a different type is passed, the data of the array is cast to the string type, and the function returns a string consisting of the unique characters from the original string.

Example

```
distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))
```

Example

```
distinct_items(DeviceCustomString1)
```

sort_items

Returns a sorted list of array elements.

You must specify the parameters in the following sequence:

1. Expression that returns the object of the sorting
2. Sorting order. Possible values: `asc`, `desc`. If the parameter is not specified, the default value is `asc`.

The function returns the sorted list of array elements if the passed array belongs to one of the following types:

- array of integers
- array of floats
- array of strings

For a boolean array, the function returns the list of array elements in the original order.

If an array of a different type is passed, the data of the array is cast to the string type, and the function returns a string of sorted characters.

Example

```
sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')
```

Example

```
sort_items(DeviceCustomString1)
```

item

Returns the array element with the specified index or the character of a string with the specified index if an array of integers, floats, strings, or boolean values is passed.

You must specify the parameters in the following sequence:

1. Expression that returns the object of the indexing
2. Expression that returns the index of the element or character

At least two parameters must be passed to the function.

The function returns the array element with the specified index or the string character with the specified index if the index falls within the range of the array and the passed array is of one of the following types:

- array of integers
- array of floats
- array of strings
- array of booleans

If an array of a different type is passed and the index falls within the range of the array, the data is cast to the string type, and the function returns the string character with the specified index. If an array of a different type is passed and the index is outside the range of the array, the function returns an empty string.

Example

```
sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')
```

Example

```
sort_items(DeviceCustomString1)
```

Operations with strings

to_lower

Converts characters in a string to lowercase. Supported for standard fields and extended event schema fields of the `string` type.

A string can be passed as a string, field name or variable.

```
Example
to_lower(SourceUserName)
```

```
Example
to_lower('SomeText')
```

```
Example
to_lower($otherVariable)
```

to_upper

Converts characters in a string to uppercase. Supported for standard fields and extended event schema fields of the `string` type.

A string can be passed as a string, field name or variable.

```
Example
to_upper(SourceUserName)
```

```
Example
to_upper('SomeText')
```

```
Example
to_upper($otherVariable)
```

append

Adds characters to the end of a string. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string
2. Added string

Strings can be passed as a string, field name or variable.

```
Example
append(Message, '123')
```

Result: the string `123` is appended to the end of the string value of the `Message` field

```
Example
append($otherVariable, 'text')
```

Result: the string `123` is appended to the end of the string value of the `otherVariable` variable.

```
Example

append(Message, $otherVariable)
```

Result: the string from the `otherVariable` variable is appended to the end of the string value of the `Message` field.

prepend

Adds characters to the beginning of a string. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string
2. Added string

Strings can be passed as a string, field name or variable.

```
Example

prepend(Message, '123')
```

Result: the string `123` is prepended to the end of the string value of the `Message` field

```
Example

prepend($otherVariable, 'text')
```

Result: the string `123` is prepended to the end of the string value of the `otherVariable` variable.

```
Example

prepend(Message, $otherVariable)
```

Result: the string from the `otherVariable` variable is prepended to the end of the string value of the `otherVariable` variable.

substring

Returns a substring from a string. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string.
2. Substring start position (natural number or 0).
3. Substring end position (optional).

Strings can be passed as a string, field name or variable. If the position number is greater than the original data string length, an empty string is returned.

```
Example
substring(Message, 2)
```

Result: part of the string value of the `Message` field is returned (from the third characters to the end).

```
Example
substring($otherVariable, 2, 5)
```

Result: part of the string value of the `otherVariable` variable is returned (from the third to the sixth character).

```
Example
substring(Message, 0, len(Message) - 1)
```

Result: the entire string value of the `Message` field is returned, except the last character.

index_of

Returns the byte offset of a character or substring in a string; the first character in the string has index 0. If the function does not find the substring, the function returns a negative value.

If the string has non-ASCII characters, the returned byte offset will not correspond to the number of characters preceding the substring you are searching for.

The function accepts the following parameters:

- As source data, an event field, another variable, or a constant.
- Any expression out of those that are available in local variables.

To use this function, you must specify the parameters in the following order:

1. Character or substring whose position you want to find.
2. String to be searched.

```
Example
index_of('@', SourceUserName)
```

Result: the `SourceUserName` field is searched for the `@` character. The `SourceUserName` field contains the `user@example.com` string. Result = 4. The function returns the index of the first occurrence of the character in the string. The first character in the string has index 0.

```
Example
index_of('m', SourceUserName)
```

Result: the `SourceUserName` field is searched for the `m` character. The `SourceUserName` field contains the `user@example.com` string. Result = 8. The function returns the index of the first occurrence of the character in the string. The first character in the string has index 0.

last_index_of

Returns the position of the last occurrence of a character or substring in a string; the first character in the string has index 0. If the function does not find the substring, the function returns `-9223372036854775808`.

The function accepts the following parameters:

- As source data, an event field, another variable, or a constant.
- Any expression out of those that are available in local variables.

To use this function, you must specify the parameters in the following order:

1. Character or substring whose position you want to find.
2. String to be searched.

Example

```
last_index_of('m', SourceUserName)
```

Result: the `SourceUserName` field is searched for the `m` character. The `SourceUserName` field contains the `user@example.com` string. Result = 15. The function returns the index of the last occurrence of the character in the string. The first character in the string has index 0.

tr

Removes the specified characters from the beginning and end of a string. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string.
2. Substring to be deleted from the beginning and end of the original string (optional)

Strings can be passed as a string, field name or variable. If you do not specify a string to be deleted, spaces will be removed from the beginning and end of the original string.

Example

```
tr(Message)
```

Result: spaces removed from the beginning and end of the string from the `Message` field.

Example

```
tr($otherVariable, '_')
```

Result: if the `otherVariable` variable has the `_test_` value, the string `test` is returned.

```
Example
tr(Message, '@example.com')
```

Result: if the `Message` event field contains the string `user@example.com`, the string `user` is returned.

replace

Replaces all occurrences of character sequence **A** with character sequence **B** in a string. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string.
2. Search string: sequence of characters to be replaced.
3. Replacement string: sequence of characters to replace the search string.

Strings can be passed as an expression.

```
Example
replace(Name, 'UserA', 'UserB')
```

Result: returns a string from the `Name` event field in which all occurrences of `UserA` are replaced with `UserB`.

```
Example
replace($otherVariable, ' text ', '_text_')
```

Result: returns a string from `otherVariable` in which all occurrences of `' text '` are replaced with `'_text_'`.

regexp_replace

Replaces a sequence of characters that matches a regular expression with a sequence of characters and regular expression capturing groups. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string.
2. Search string: regular expression.
3. Replacement string: sequence of characters to replace the search string, and IDs of the regular expression capturing groups. A string can be passed as an expression.

Strings can be passed as a string, field name or variable. Unnamed capturing groups can be used.

In regular expressions used in variable functions, each backslash character must be additionally escaped. For example, `^example\\\\` must be used instead of the regular expression `^example\\`.

```
Example

regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')
```

Result: returns a string from the `SourceAddress` event field in which the text `newIP` is inserted before the IP addresses. In addition, the last digits of the address are replaced with `10`.

regexp_capture

From the original string, gets the result matching the regular expression. Supported for standard fields and extended event schema fields of the `string` type.

You must specify the parameters in the following sequence:

1. Original string.

2. Search string: regular expression.

Strings can be passed as a string, field name or variable. Unnamed capturing groups can be used.

In regular expressions used in variable functions, each backslash character must be additionally escaped. For example, `^example\\\\` must be used instead of the regular expression `^example\\`.

```
Example

regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')
```

```
Example values

Message = 'Access from 192.168.1.1 session 1'
Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'
```

Result:

`'192.168.1.1'`

`'45.45.45.45'`

template

Returns the string specified in the function, with variables replaced with their values. The `template` function can be used in one of two ways:

- With one argument: you can use field names to substitute values in the template.
- With multiple arguments: the zero-based index of the argument is used to substitute values.

Example

```
template('Message text: {{.Message}}')
```

Example

```
template('Name in lower case: {{index . 0}}.Name in upper case: {{index . 1}}', to_lower(Name), to_upper(Name))
```

Operations with timestamps

now function

Gets a timestamp in `epoch` format. Runs with no arguments.

Example

```
now()
```

extract_from_timestamp

Gets atomic time representations (year, month, day, hour, minute, second, day of the week) from fields and variables with time in the `epoch` format.

The parameters must be specified in the following sequence:

1. Event field of the `timestamp` type, or variable.
2. Notation of the atomic time representation. This parameter is case sensitive.
   Possible variants of atomic time notation:
   - y refers to the year in number format.
   - M refers to the month in number notation.
   - d refers to the number of the month.
   - wd refers to the day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h refers to the hour in 24-hour format.
   - m refers to the minutes.
   - s refers to the seconds.
3. Time zone designation (optional).

The parameter can be specified as a string (for example, `Europe/Moscow`) or as a variable (`$timezone`). The variable must be previously declared in the local variables of the correlation rule. The value of the variable must contain a string identifier for the time zone. You can also use variables derived from other variables and dictionary values.

If this parameter is not specified, the time is calculated in UTC format.

Example

```
extract_from_timestamp(Timestamp, 'wd')
```

Example

```
extract_from_timestamp(Timestamp, 'h')
```

Example

```
extract_from_timestamp($otherVariable, 'h')
```

Example

```
extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')
```

Example

```
extract_from_timestamp(Timestamp, 'h', $timezone)
```

Example of using a variable from a dictionary

```
$key_timezone = 'timezone'
$timezone = dict('UEBA.Timezone', $key_timezone)
extract_from_timestamp(EndTime, 'h', $timezone)
```

In this example, the `$timezone` variable is generated based on another variable and a dictionary value and is used as the `timezone` parameter.

parse_timestamp

Converts the time from RFC3339 format (for example, `2022-05-24 00:00:00`, `2022-05-24 00:00:00+0300`) to `epoch` format.

Example

```
parse_timestamp(Message)
```

Example

```
parse_timestamp($otherVariable)
```

format_timestamp

Converts the time from `epoch` format to RFC3339 format.

The parameters must be specified in the following sequence:

1. Event field of the `timestamp` type, or variable.
2. Time format notation: RFC3339.
3. (optional) Time zone notation. If this parameter is not specified, the time is calculated in UTC format.

Example

```
format_timestamp(Timestamp, 'RFC3339')
```

Example

```
format_timestamp($otherVariable, 'RFC3339')
```

Example

```
format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')
```

truncate_timestamp

Rounds the time in `epoch` format. After rounding, the time is returned in `epoch` format. Time is rounded down.

The parameters must be specified in the following sequence:

1. Event field of the `timestamp` type, or variable.
2. Rounding parameter:
   - 1s rounds to the nearest second.
   - 1m rounds to the nearest minute.
   - 1h rounds to the nearest hour.
   - 24h rounds to the nearest day.
3. (optional) Time zone notation. If this parameter is not specified, the time is calculated in UTC format.

Example

```
truncate_timestamp(Timestamp, '1m')
```

Example of value to be rounded: 1654631774175 (7 June 2022, 19:56:14.175).

Result: 1654631760000 (7 June 2022, 19:56:00).

Example

```
truncate_timestamp($otherVariable, '1h')
```

Example of value to be rounded: 1654631774175 (7 June 2022, 19:56:14.175).

Result: 1654628400000 (7 June 2022, 19:00:00).

```
Example
truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')
```

Example of value to be rounded: 1654631774175 (7 June 2022, 19:56:14.175).

Result: 1654560000000 (7 June 2022, 0:00:00).

time_diff

Gets the time interval between two timestamps in `epoch` format.

The parameters must be specified in the following sequence:

1. Interval end time. Event field of the `timestamp` type, or variable.
2. Interval start time. Event field of the `timestamp` type, or variable.
3. Time interval notation:
   - ms refers to milliseconds.
   - s refers to seconds.
   - m refers to minutes.
   - h refers to hours.
   - d refers to days.

```
Example
time_diff(EndTime, StartTime, 's')
```

```
Example
time_diff($otherVariable, Timestamp, 'h')
```

```
Example
time_diff(Timestamp, DeviceReceiptTime, 'd')
```

Mathematical operations

These are comprised of basic mathematical operations and functions.

Basic mathematical operations

Supported for extended event schema fields of the `integer` and `float` types.

Operations:

- Addition
- Subtraction
- Multiplication
- Division
- Modulo division

Parentheses determine the sequence of actions.

Available arguments:

- Numeric event fields
- Numeric variables
- Real numbers

  When modulo dividing, only natural numbers can be used as arguments.

Usage constraints:

- Division by zero returns zero.
- Mathematical operations on a number and a string return the number unchanged. For example, `1 + abc` returns `1`.
- Integers resulting from operations are returned without a dot.

Examples for `(Type=3; otherVariable=2; Message=text)`	Result
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

round

Rounds numbers. Supported for extended event schema fields of the `integer` and `float` types.

Available arguments:

- Numeric event fields
- Numeric variables
- Numeric constants

Examples for `(DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)`	Result
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

ceil

Rounds a number up. Supported for extended event schema fields of the `integer` and `float` types.

Available arguments:

- Numeric event fields
- Numeric variables
- Numeric constants

Examples for `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Result
`ceil(DeviceCustomFloatingPoint1)`	8
`ceil($otherVariable)`	9

floor

Rounds a number down. Supported for extended event schema fields of the `integer` and `float` types.

Available arguments:

- Numeric event fields
- Numeric variables
- Numeric constants

Examples for `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Result
`floor(DeviceCustomFloatingPoint1)`	7
`floor($otherVariable)`	8

abs

Gets the absolute value of a number. Supported for extended event schema fields of the `integer` and `float` types.

Available arguments:

- Numeric event fields
- Numeric variables
- Numeric constants

Examples for `(DeviceCustomNumber1=-7; otherVariable=-2)`	Result
`abs(DeviceCustomFloatingPoint1)`	7
`abs($otherVariable)`	2

pow

Raises a number to a power. Supported for extended event schema fields of the `integer` and `float` types.

The parameters must be specified in the following sequence:

1. Base—real numbers.
2. Exponent—natural numbers or real numbers.

Available arguments:

- Numeric event fields
- Numeric variables
- Numeric constants

Example

```
pow(DeviceCustomNumber1, DeviceCustomNumber2)
```

Example

```
pow($otherVariable, DeviceCustomNumber1)
```

str_join

Joins multiple strings into one using a separator. Supported for extended event schema fields of the `integer` and `float` types.

The parameters must be specified in the following sequence:

1. Separator. String.

2. String 1, string 2, string N. At least two expressions.

```
Example

str_join('|', to_lower(Name), to_upper(Name), Name)
```

Result: string.

conditional

Has one value if a condition is satisfied and a different value if the condition is not satisfied. Supported for extended event schema fields of the `integer` and `float` types.

The parameters must be specified in the following sequence:

1. Condition: string; the syntax is similar to the conditions of the WHERE clause in SQL. You can use the functions of the KUMA variables and references to other variables in a condition.

2. The value if the condition is satisfied: expression.

3. The value if the condition is not satisfied: expression.

Supported operators:

- `AND`
- `OR`
- `NOT`
- `=`
- `!=`
- `<`
- `<=`
- `>`
- `>=`
- `LIKE`

  A RE2 regular expression is passed, rather than an SQL expression.

- `ILIKE`

  A RE2 regular expression is passed, rather than an SQL expression.

- `BETWEEN`

- `IN`
- `IS NULL`

  Checks for an empty value, such as 0 or an empty string.

Example

```
conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')
```

Example

```
conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')
```

Example

```
conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')
```

In all examples, the value depends on arguments 2 and 3.

Operations for extended event schema fields

For extended event schema fields of the `string` type, the following functions are supported:

- `len`
- `to_lower`
- `to_upper`
- `append`
- `prepend`
- `substring`
- `tr`
- `replace`
- `regexp_replace`
- `regexp_capture`

For extended event schema fields of the `integer` or `float` type, the following simple mathematical operations are supported:

- `round`
- `ceil`
- `floor`
- `abs`

- `pow`
- `str_join`
- `conditional`

For extended event schema fields of the `array of integers`, `array of floats`, and `array of strings` types, KUMA supports the following functions:

- Get the i-th element of the array.

  Example
  ```
  item(<type>.someStringArray)
  ```

- Get an array of values.

  Example
  ```
  <type>.someStringArray
  ```

  Returns `["string1", "string2", "string3"]`.

- Get the count of elements in an array.

  Example
  ```
  len(<type>.someStringArray)
  ```

  Returns `["string1", "string2"]`.

- Get unique elements from an array.

  Example
  ```
  distinct_items(<type>.someStringArray)
  ```

- Generate a TSV string of array elements.

  Example
  ```
  to_string(<type>.someStringArray)
  ```

- Sort the elements of the array.

  Example
  ```
  sort_items(<type>.someStringArray)
  ```

In the examples, instead of `<type>`, you must specify the array type: NA for an array of integers, FA for an array of floats, SA for an array of strings.

For fields of the `array of integers` and `array of floats` types, the following functions are supported:

- `math_min` returns the minimum element of an array.

  Example
  ```
  math_min(NA.NumberArray)
  ```

  Example
  ```
  math_min(FA.FloatArray)
  ```

- `math_max` returns the maximum element of an array

  Example
  ```
  math_max(NA.NumberArray)
  ```

  Example
  ```
  math_max(FA.FloatArray)
  ```

- `math_avg` returns the average value of an array.

  Example
  ```
  math_avg(NA.NumberArray)
  ```

  Example
  ```
  math_avg(FA.FloatArray)
  ```

Declaring variables

To declare variables, they must be added to a correlator or correlation rule.

To add a global variable to an existing correlator:

1. In the KUMA web interface, under **Resources** → **Correlators**, select the resource set of the relevant correlator. This opens the Correlator Installation Wizard.
2. Select the **Global variables** step of the Installation Wizard.
3. Click the **Add variable** button and specify the following parameters:
   - In the **Variable** window, enter the name of the variable.

     Variable naming requirements

     - Must be unique within the correlator.
     - Must contain 1 to 128 Unicode characters.

- Must not begin with the character $.
- Must be written in camelCase or CamelCase.

- In the **Value** window, enter the variable function.

  When entering functions, you can use autocomplete as a list of hints with possible function names, their brief description and usage examples. You can select a function from the list and insert it together with its list of arguments into the input field.

  To display the list of all hints in the field, press **`Ctrl+Space`**. Press **`Enter`** to select a function from the list. Press **`Tab`** to go to the next argument in the list of arguments of the selected function.

  Description of variable functions.

Multiple variables can be added. Added variables can be edited or deleted by using the × icon.

4. Select the **Setup validation** step of the Installation Wizard and click **Save**.

A global variable is added to the correlator. It can be queried like an event field by inserting the $ character in front of the variable name. The variable will be used for correlation after restarting the correlator service.

To add a local variable to an existing correlation rule:

1. In the KUMA web interface, under **Resources** → **Correlation rules**, select the relevant correlation rule.

   The correlation rule settings window opens. The parameters of a correlation rule can also be opened from the correlator to which it was added by proceeding to the **Correlation** step of the Installation Wizard.

2. Click the **Selectors** tab.

3. In the selector, open the **Local variables** tab, click the **Add variable** button and specify the following parameters:

   - In the **Variable** window, enter the name of the variable.

     Variable naming requirements

     - Must be unique within the correlator.
     - Must contain 1 to 128 Unicode characters.
     - Must not begin with the character $.
     - Must be written in camelCase or CamelCase.

   - In the **Value** window, enter the variable function.

     When entering functions, you can use autocomplete as a list of hints with possible function names, their brief description and usage examples. You can select a function from the list and insert it together with its list of arguments into the input field.

     To display the list of all hints in the field, press **`Ctrl+Space`**. Press **`Enter`** to select a function from the list. Press **`Tab`** to go to the next argument in the list of arguments of the selected function.

     Description of variable functions.

Multiple variables can be added. Added variables can be edited or deleted by using the × icon.

For standard correlation rules, repeat this step for each selector in which you want to declare variables.

4. Click **Save**.

   The local variable is added to the correlation rule. It can be queried like an event field by inserting the $ character in front of the variable name. The variable will be used for correlation after restarting the correlator service.

Added variables can be edited or deleted. If the correlation rule queries an undeclared variable (for example, if its name has been changed), an empty string is returned.

If you change the name of a variable, you will need to manually change the name of this variable in all correlation rules where you have used it.

Adding a temporary exclusion list for a correlation rule

Users that do not have the rights to edit correlation rules in the KUMA web interface, can create a temporary list of exclusions (for example, create exclusions for false positives when managing alerts). A user with the rights to edit correlation rules can then add the exclusions to the rule and remove them from the temporary list.

To add exclusions to a correlation rule when managing alerts:

1. Go to the **Alerts** section and select an alert.

2. Click the **Find in events** button.

   Events of the alert are displayed on the events page.

3. Open the correlation event.

   This opens the event card in which each field has a ⌄ (arrow) button that lets you add an exclusion.

4. Click the ⌄ button and select **Add to exclusions** .

   A sidebar is displayed, containing the following fields: **Correlation rule**, **Exclusion**, **Alert**, **Comment**.

5. Click the **Create** button.

   The exclusion rule is added.

The exclusion is added to the temporary list. This list is available to anyone with rights to read correlation rules: in the **Resources** → **Correlation rules** section, in the toolbar of the rule list, click the **List of exclusions** button. If you want to view the exclusions of a specific rule, open the card of the rule and select the **Exclusions** tab.

The exclusion list contains entries with the following parameters:

- `Exclusion`

  Exclusion condition.

- `Correlation rule`

  Name of the correlation rule.

- `Alert`

  Name of the alert from which the exclusion was added.

- `Tenant`

  The tenant to which the rule and the exclusion apply.

- `Condition`

  Generated automatically based on the selected field of the correlation event.

- `Creation date`

  Date and time when the exclusion was added.

- `Expires`

Date and time when the exclusion will be automatically removed from the list.

- `Created`

  Name of the user that added the exclusion.

- `Comment`

After the exclusion is added, by default, the correlation rule takes the exclusion into account for 7 days. In the **Settings** → **Other** → **General** section, you can configure the duration of exclusions by editing the `corr_rule_exclusion_ttl_hours` parameter in the **Core properties** section. You can configure the lifetime of exclusions in hours and days. The minimum value is 1 hour, the maximum is 365 days. This setting is available only for users with the Main administrator role.

For fields from base events to be propagated to correlation events, these fields must be specified in the card of the correlation rule on the **General** tab, in the **Propagated fields** field. If the fields of base events are not mapped to the correlation event, these fields cannot be added to exclusions.

To remove exclusions from a correlation rule:

1. Go to the **Resources** → **Correlation rules** section.

2. In the toolbar of the rule list, click **List of exclusions** button.

   This opens the window with the list of exclusions.

3. Select the exclusions that you want to delete and click the **Delete** button.

Exceptions are deleted from the correlation rule.

KUMA generates an audit event whenever an exception is created or deleted. You can view the changes of event settings in the Event details window.

Predefined correlation rules

The KUMA distribution kit includes correlation rules listed in the table below.

Predefined correlation rules

Correlation rule name	Description
[OOTB] KATA alert	Used for enriching KATA events.
[OOTB] Successful Bruteforce	Triggers when a successful authentication attempt is detected after multiple unsuccessful authentication attempts. This rule works based on the events of the sshd daemon.

[OOTB][AD] Account created and deleted within a short period of time	Detects instances of creation and subsequent deletion of accounts on Microsoft Windows hosts.
[OOTB][AD] An account failed to log on from different hosts	Detects multiple unsuccessful attempts to authenticate on different hosts.
[OOTB][AD] Membership of sensitive group was modified	Works based on Microsoft Windows events.
[OOTB][AD] Multiple accounts failed to log on from the same host	Triggers after multiple failed authentication attempts are detected on the same host from different accounts.
[OOTB][AD] Successful authentication with the same account on multiple hosts	Detects connections to different hosts under the same account. This rule works based on Microsoft Windows events.
[OOTB][AD] The account added and deleted from the group in a short period of time	Detects the addition of a user to a group and subsequent removal. This rule works based on Microsoft Windows events.
[OOTB][Net] Possible port scan	Detects suspected port scans. This rule works based on Netflow, Ipfix events.

Correlation rule packages

Downloadable files describe the correlation rules included in the KUMA 4.6 distribution. It provides the scenarios covered by rules, the conditions of their use, and the necessary sources of events.

You can import correlation rules into KUMA. See the *Resource import* Help section.

Resources from the repository are imported from the repository in the language specified in the **KUMA resources localization** setting in the KUMA Core settings section.

You can add imported correlation rules to correlators that your organization uses. See the Help section *Step 3. Correlation*.

Download the description of KSC Package correlation rules

Download the description of KSMG Package correlation rules

Download the description of KATA Package correlation rules

Download the description of KUMA Package correlation rules

Download the description of Network Package correlation rules

Download the description of PCIDSS Package correlation rules

Download a description of SOC Content for KUMA correlation rules

Download the description of UEBA Package correlation rules

Download the description of XDR Package correlation rules

Download the description of PostgreSQL Package correlation rules

Description of correlation rule packages

The distribution kit of Kaspersky Unified Monitoring and Analysis Platform 4.6 includes the correlation rule packages listed in the table below.

Package name	Description
[OOTB] SOC Content - RU [OOTB] SOC Content - ENG	Correlation rule packages for KUMA versions 2.1 or later with Russian and English localization. This package is no longer supported.
[OOTB] SOC Content - RU for KUMA 3.2 [OOTB] SOC Content - ENG for KUMA 3.2	Correlation rule packages for KUMA versions 3.2 or later with Russian and English localization. The rules contain information about MITRE ATT&CK matrix coverage.
[OOTB] KUMA package - RU [OOTB] KUMA package - ENG	Correlation rules package for monitoring KUMA events. The correlation rules allow detecting potentially dangerous actions in the system based on internal audit events. The package is available for KUMA versions 3.2 or later with Russian and English localization. Solution audit events are used to detect anomalies in user behavior, such as failed login attempts, connections from non-typical IP addresses, and password brute-force attempts. Attempts to change solution settings, including manipulation of accounts and other parameters, are also monitored. Such actions may indicate unauthorized access or bypassing security mechanisms to conduct further attacks on the corporate infrastructure. This package also includes rules for monitoring the health of services. For the rules to work correctly, make sure your audit settings provide for a sufficient level of detail in event logs.
[OOTB] KSC Package - RU [OOTB] KSC Package - ENG	Package of correlation rules for monitoring Kaspersky Security Center events. The package is available for KUMA versions 3.2 or later with Russian and English localization. Allows detecting potentially dangerous actions in the system based on internal audit events. For correlation rules to work properly, make sure your audit settings provide for a sufficient level of detail in event logs. The correlation rules package works on events that are collected via the Kaspersky Security Center database. The rules contain information about MITRE ATT&CK matrix coverage.
[OOTB] KSMG Package - RU [OOTB] KSMG Package - ENG	Package of correlation rules for monitoring Kaspersky Security Mail Gateway events. The package is available for KUMA versions 3.2 or later with Russian and English localization. Allows detecting potentially dangerous actions in the mail traffic protection system system based on internal audit events. For the rules to work properly, make sure your audit settings provide for a sufficient level of detail in event logs. The audit settings of Kaspersky Secure Mail Gateway are located in the **Settings** → **Logs and events** → **Events** section. In the **Audit events** section, select **Audit log level** → **Log audit events and modified parameters**. Notes: • The package of rules works on events in CEF format. • To export events to the SIEM system, you need the Kaspersky Secure Mail Gateway log in CEF (local2) format. The rules contain information about MITRE ATT&CK matrix coverage.
[OOTB] KATA package - RU [OOTB] KATA package - ENG	The correlation rules package for monitoring Kaspersky Anti Targeted Attack (KATA) events allows detecting potentially dangerous activity in the system based on internal audit events. The package is available for KUMA versions 3.2 or later with Russian and English localization. Application audit events are used to detect anomalies in user behavior, such as failed login attempts, connections from non-typical IP addresses, and password brute-force attempts. Attempts to change application settings, including manipulation of accounts and disabling of detection rules, are also monitored. Such actions may indicate unauthorized access or bypassing security mechanisms to conduct further attacks on the corporate infrastructure. For the rules to work correctly, make sure your audit settings provide for a sufficient level of detail in event logs.
[OOTB] Network Package - RU [OOTB] Network Package - ENG	Package of correlation rules aimed at detecting network activity anomalies, for KUMA versions 3.2 and later with Russian and English localization. The rules contain information about MITRE ATT&CK matrix coverage. The package also contains dashboards.
[OOTB] PCIDSS Package - RU [OOTB] PCIDSS Package - ENG	Package of correlation rules aimed at compliance with the PCI DSS standard. The package is available for KUMA versions 3.2 or later with Russian and English localization. This package also contains dashboards. For the resource set to work correctly, you need to add the **S.Compliance_PCIDSS_Requirements** extended event schema field in the **Settings** → **Other** → **Extended event schema fields**. The rules contain information about MITRE ATT&CK matrix coverage.
[OOTB] XDR package - RU [OOTB] XDR package - ENG	This package contains a set of resources for detecting advanced attacks in the infrastructure. The package is available for KUMA version 3.2 or later with Russian localization. It can help detect phishing (which is, according to Kaspersky MDR, the most popular vector of initial access), but also virus infection, defense evasion, payload delivery and attempts to bypass protective equipment, delivery and launch, persistence, reconnaissance, lateral movement, and various methods of communication with a command and control server. The rules can be applied to events from Kaspersky software (EDR, KSC, KSMG) as well as events from Windows operating systems. The rules contain information about MITRE ATT&CK matrix coverage.

Package name	Description
[OOTB] UEBA package - RU [OOTB] UEBA package - ENG	Beta version of the correlation rule package. This correlation rule package aims to detect abnormal behavior of an account or workstation on a corporate network. The package is available for KUMA versions 3.2 or later with Russian and English localization. It builds adaptive models of normal behavior based on accumulated historical data (the data collection period can be configured, one month being the default). These models are used to calculate statistical indicators that minimize false positives and effectively identify potentially dangerous deviations. Sources of data: Windows OS, NetFlow, Cisco, Solar Proxy events. Notes: • Collection rules can be adapted to specific information security tools and telemetry sources. • Event enrichment with DNS data is critical to maximizing the effectiveness of the package. • Rules may affect the performance of the correlator. • We recommend using these rules in KUMA version 4.0 and higher. The rules contain information about MITRE ATT&CK matrix coverage.
[OOTB] NCCCI package - RU for KUMA 4.0	This package includes a set of dashboards and report templates that visualize detailed information about violations classified by categories and types of security incidents from the National Computer Incident Response and Coordination Center (NCIRCC). The visualization is based on the values of the S.Compliance_NCCCI_IncidentClassification field, which is automatically populated by an enrichment rule for rules from the SOC package. Before importing the visualization package, you must create the S.Compliance_NCCCI_IncidentClassification extended event schema field of the string type or check to make sure that it exists. This package also contains dashboards.
[OOTB] FSTEC package - RU for KUMA 4.0	This package includes a set of dashboards and report templates that visualize detailed information about violations of protective measures recommended by the Russian Federal Service for Technical and Export Control (FSTEC) to prevent threats and eliminate vulnerabilities in accordance with the Information Security Threat Database. The visualization is based on the values of the S.Compliance_FSTEC_ProtectiveMeasures field, which is automatically populated by an enrichment rule for rules from the SOC package. Before importing the visualization package, you must create the S.Compliance_FSTEC_ProtectiveMeasures extended event schema field of the string type or check to make sure that it exists. This package also contains dashboards.
[OOTB] PostgreSQL package - RU [OOTB] PostgreSQL package - ENG	Correlation rules package for monitoring PosgreSQL events. The correlation rules allow detecting potentially dangerous actions in the system based on internal audit events. Application audit events detect anomalies in user behavior, such as the gathering of information about user accounts, attempts to execute arbitrary code on the system, as well as writing and reading data from the file system. For correlation rules to work correctly, make sure your audit settings provide for a sufficient level of detail in event logs.

Automatic rule suppression

The SOC_package correlation rules package allows automatically suppressing the triggering of rules if the triggering frequency exceeds thresholds.

The automatic suppression option works as follows: if a rule is triggered more than 100 times in 1 minute and this behavior occurs at least 5 times in the span of 10 minutes, the rule is added to the stop list.

- When placed in the stop list for the first time, the rule is disabled for 1 hour.
- If this happens again, it is placed in the list for 24 hours.
- All subsequent occurrences place it in the list for 7 days.

The logic is described in the resources: rules, active lists, and dictionaries, which are located in the "SOC_package/System/Rule disabling by condition" directory.

You can customize settings and thresholds in accordance with your requirements.

To enable the automatic suppression option, set the **enable** setting to `1` in the "SOC_package/Integration/Rule disabling configuration" dictionary.

To disable the automatic suppression option, set the **enable** setting to `0` in the "SOC_package/Integration/Rule disabling configuration" dictionary.

By default, automatic suppression is enabled and the **enable** setting is set to `1`.

Audit events

Correlation rules from the "[OOTB] SOC Content" resource set use the audit events that are listed in the table below.

Audit events

Event source	Audit events
CheckPoint	Anti Malware, Threat Emulation
Cisco ASA, FTD, PIX	106021, 320001, 322001, 322002, 322003, 405001, 405002
CyberTrace	alert
DNS	query
KATA	TAA has tripped on events database
KSC	GNRL_EV_ATTACK_DETECTED, GNRL_EV_SUSPICIOUS_OBJECT_FOUND, GNRL_EV_VIRUS_FOUND, GNRL_EV_WEB_URL_BLOCKED, KLSRV_HOST_STATUS_CRITICAL, KLSRV_HOST_STATUS_OK, KLSRV_HOST_STATUS_WARNING
KSMG	LMS_EV_SCAN_LOGIC_AV_STATUS, LMS_EV_SCAN_LOGIC_KT_STATUS, LMS_EV_SCAN_LOGIC_CF_STATUS, LMS_EV_SCAN_LOGIC_AP_STATUS
KUMA	Correlation rule
Windows Event Log Powershell	4103, 4104
Windows Event Log Security	1102, 4624, 4625, 4656, 4657, 4662, 4663, 4672, 4688, 4697, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4768, 4769, 4771, 5136, 5140, 5145
Windows Event Log System	7036, 7045
Windows Event Log Defender	1006, 1015, 1116, 1117, 5001, 5010, 5012, 5101
Netflow, FW	Traffic log
Palo Alto	virus
auditd	ADD_USER, DEL_USER, PATH, SYSCALL, USER_AUTH, USER_LOGIN, execve

Correlation using assets and asset categories

KUMA allows you to use asset categories in correlation rules. Such correlation rules are more universal, as they cover a larger number of assets than rules targeting specific assets. For example, you can configure a correlation rule to trigger if an asset from one category is found as a source and an asset from another category is found as a target.

Configuring correlation rules using asset categories consists of the following steps:

1 Adding assets to KUMA

Assets are added to KUMA either manually or imported from other solutions, for example from Kaspersky Security Center. KUMA assigns the `AssetID` to all added assets. When an event arrives in KUMA, its fields do not contain the `AssetID` value; that is, there is no information about which assets from the list of assets added to KUMA were affected. The enrichment of events with information about assets occurs in the collector.

2 Configuring event enrichment with asset information on collectors

Since asset enrichment increases the load on the collector service, it is recommended to choose on which collectors to configure asset enrichment. This can be done based on the type and function of event sources that send events to the collector. You can configure asset enrichment on all collectors and later disable it on collectors that do not require it.

You can configure event enrichment with assets in the **Event enrichment** step when creating a collector. To do this, you need to create and configure an enrichment rule of **the asset enrichment** type. You can do this either in the **Event enrichment** step or by creating an enrichment rule in advance and then linking it to the collector.

The logic of the asset enrichment rule is as follows: When an event arrives at the collector, KUMA checks whether the `SourceAddress`, `DestinationAddress`, `DeviceAddress`, `SourceHostName`, `DestinationHostName`, and `DeviceHostName` fields are filled in. The IP address or FQDN values from these fields are then compared with the IP address and FQDN values from the properties of assets added to KUMA. Thus, matching values from the event fields and asset properties allows KUMA to determine which asset is specified in the event. Next, KUMA writes the `AssetID` value of the matched asset to one or more of the following event fields: `SourceAssetID`, `DestinationAssetID`, and `DeviceAssetID`. The events are then sent to a correlator or storage.

3 Adding asset categories

You can create asset categories to group assets into logical groups based on a shared characteristic.

4 Setting up correlation using asset categories

The correlator receives a normalized event. If `AssetID` values are specified in this event, the correlator retrieves information about the belonging of this asset to asset categories through a query to the KUMA Core database. Thus, based on this information, you can create correlation rules in which you can specify asset categories as trigger conditions.

For example, to detect an attack of attempted access by an unprivileged user to critical infrastructure elements, you can create a correlation rule and specify a filter on the **Selectors** tab:

```
SourceAssetID inCategory "Devices of unprivileged users"
AND
DestinationAssetID inCategory "Infrastructure equipment"
AND
DestinationPort = OR (22, 3389, 1433)
```

With these parameters, when an event is received indicating an attempt to access from a device in the "Devices of unprivileged users" category to a device in the "Infrastructure equipment" category on ports 22, 3389, or 1433, KUMA performs the following actions:

1. The collector identifies assets that correspond to the IP addresses of the source and destination devices.

   a. The correlator performs the following actions in sequence:

   b. Determines which categories these assets belong to.

   c. Applies the filter specified in the correlation rule.

   d. Creates a correlation event, when the filter conditions are met.

2. An alert is created in the web interface.

❺ Response

You can start tasks on specific assets manually in the asset information window or automatically using response rules.

MITRE ATT&CK techniques and tactics

> All operations with MITRE ATT&CK techniques and tactics become available only after importing the list of MITRE ATT&CK techniques.

KUMA can:

- Enrich correlation events with information about MITRE ATT&CK techniques and tactics.

  Tactic and Technique fields of the event data model are used for this purpose. When generating a correlation event, these fields can be populated with relevant data for later use. For example, when a new alert is received with MITRE ATT&CK markup, you can open the MITRE ATT&CK website and read about the techniques and tactics to learn when, how, and why attackers might use these techniques, how to detect them, and how to mitigate risks — all of this can help you develop a response plan. You can also build reports and dashboards based on alerts and techniques detected in the infrastructure. If you are using correlation rules from SOC_package and want to customize the enrichment of correlation events with information about MITRE ATT&CK techniques and tactics, add the MITRE enrichment rules to the correlator.

- Assess the coverage of the MITRE ATT&CK matrix by your correlation rules.

  In this case, the general correlation rule parameters are used, which allow associating MITRE techniques with each rule. This parameter is used to describe the rule itself and this data is not passed to the correlation rule or alert in any way. Associating techniques and tactics with correlation rules lets you analyze the MITRE ATT&CK matrix coverage, focusing on the most relevant techniques for your specific infrastructure.

If you want to assess the coverage of the MITRE ATT&CK matrix by your correlation rules:

1. Download the list of techniques from the official MITRE ATT&CK repository and import it into KUMA.
2. Map MITRE ATT&CK techniques to correlation rules.
3. Export correlation rules to MITRE ATT&CK Navigator.

As a result, you can visually assess the coverage of the MITRE ATT&CK matrix.

- Visualization of the MITRE ATT&CK matrix coverage by Kaspersky products.

Importing the list of MITRE ATT&CK techniques

Only a user with the General Administrator role can import the list of MITRE ATT&CK techniques.

To import the list of MITRE ATT&CK techniques:

1. Download the list of MITRE ATT&CK techniques from the GitHub portal.

   KUMA 4.6 only supports the list of MITRE ATT&CK techniques starting with version 14.2; the recommended version is 19.2.

2. In the KUMA web interface, go to the **Settings** → **Other** → **General** section.
3. In the **MITRE Techniques List Settings**, click **Import from file**.

   This opens the file selection window.

4. Select the downloaded MITRE ATT&CK technique list and click **Open**.

   This closes the file selection window.

The list of MITRE ATT&CK techniques is imported into KUMA. The list of imported techniques and the version of the MITRE ATT&CK technique list will be displayed by clicking **View list**.

Adding MITRE enrichment rules to the correlator

The **MITRE Technique** and **MITRE Tactics** enrichment rules are only intended for and applied to enrichment of correlation rules imported from the SOC_package. If custom correlation rules are used in the correlator, adding the **MITRE Technique** and **MITRE Tactics** enrichment rules does not automatically enrich these.

To add a MITRE enrichment rule:

1. Make sure that the list of MITRE techniques has been imported.
2. In the **Resources and services** → **Correlators** section in KUMA, click **Add** to create a correlator or select an existing correlator from the list to enter the settings editing mode.
3. In the Correlator Installation Wizard, on the **Enrichment** step, click **Add enrichment**.
4. This opens the **Enrichment** window; in that window, in the **Enrichment rule** drop-down list, select the **MITRE Technique** and **MITRE Tactics** rules.

5. Save the correlator settings.

6. If you have created a correlator, you must install the correlator service on the host. If you edited the settings of an active correlator, you must restart the correlator service.

MITRE Technique and **MITRE Tactics** enrichment rules are added.

Mapping MITRE ATT&CK techniques to correlation rules

To map MITRE ATT&CK techniques to correlation rules:

1. In the KUMA web interface, go to the **Resources** → **Correlation rules** section.

2. Click the name of the correlation rule to open the correlation rule editing window.

   This opens the correlation rule editing window.

3. On the **General** tab, clicking the **MITRE techniques** field opens a list of available techniques. For the convenience of searching, a filter is provided, in which you can enter the name of a technique or the ID of a technique or tactic. One or more MITRE ATT&CK techniques are available for linking to a correlation rule.

4. Click **Save**.

The MITRE ATT&CK techniques are mapped to the correlation rule. In the web interface, in the **Resources** → **Correlation rules** section, the **MITRE techniques** column of the edited rule displays the ID of the selected technique, and when you hover over the item, the full name of the technique is displayed, including the ID of the technique and tactic.

Exporting correlation rules to MITRE ATT&CK Navigator

To export correlation rules with mapped techniques to MITRE ATT&CK Navigator:

1. In the KUMA web interface, go to the **Resources** → **Correlation rules** section.

2. Click the **...** button in the upper-right corner.

3. In the drop-down list, click **Export to MITRE ATT&CK Navigator**.

4. This opens a window; in that window, select the correlation rules that you want to export.

5. Click **OK**.

   A file with exported rules is downloaded to your computer.

6. Upload the file from your computer to MITRE ATT&CK Navigator to assess the coverage of the MITRE ATT&CK matrix.

You can assess the coverage of the MITRE ATT&CK matrix.

Sigma rules converter

The Sigma rule converter converts correlation rules into a format supported by KUMA and facilitates importing simple rules to be refined by an analyst.

The list of operating systems that support the Sigma rule converter is given in the Software requirements section.

To use the Sigma rule converter to convert correlation rules:

1. Install the Sigma rule converter. The following installation options are available:

   Installing the Sigma rule converter using docker and bash

   This installation method is suitable for local installation of the converter web interface.

   Installation requires the latest versions of bash and docker. For detailed information about deploying bash and docker, refer to the official documentation.

   Astra Linux 1.7 is not supported.

   To install a converter:

   1. Enter the directory with the extracted archive and execute one of the following commands:

      - To install the converter on host `0.0.0.0:8000`, run the following command:

        ```
        ./run.sh
        ```

      - To install the converter on host `0.0.0.0` and another port, for example, `8888`, run the following command:

        ```
        ./run.sh <port>
        ```

        where:

        `<port>` is the port (the default port is `8000`).

      - To install the converter on host `127.0.0.1:9999`, run the following command:

        ```
        ./run.sh <IP address>:<port>
        ```

        where:

        - `<IP address>`

          in the range of
          is the IP address of the listening interface.

          `0.0.0.0`
          . Specify

          `127.0.0.1`
          to run only on the local interface.

        - `<port>`

          is the port.

   The converter is installed.

   Installing the Sigma rule converter in an environment that allows running docker images

This installation method uses the provided container and lets you create a systemd service and deploy the web interface using Kubernetes.

Any container tool will do, such as docker, podman, or cri-o. Installation involves downloading the container image and then running the image with a port specified.

To install the converter using podman:

1. Download the container image:

```
podman load --input "kuma-sigma-converter-x.x.x.tar
```

2. Run the image in one of the following ways:

   - By running the following command:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
     ```

     Wait for the command to finish or to become idle. Do not press **Ctrl**+**C** before the installation process has finished or you get an explicit prompt to abort the installation

   - Run in the background:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
     ```

The converter is installed.

Installing the Sigma rule converter using Python 3.10 or later

This installation method is the most flexible and suitable for experienced users because it lets you adapt the converter to your specific needs. Unlike other methods, this method requires an internet connection to download Python packages.

To install a converter:

1. Make sure you have Python 3.10 or later installed.

2. Install poetry for Python dependency management. For Ubuntu or Debian, you can use the package manager:

```
sudo apt-get update
sudo apt install pipx
pipx install poetry
```

3. Use poetry to configure and run the web interface of the Sigma rule converter:

```
cd sigconverter.io
poetry install
poetry run ./run.py
```

4. In the browser, navigate to the host where the web interface of the Sigma rule converter is installed. For a local installation, the address is `http://127.0.0.1:8000` or `http://0.0.0.0:8000`.

5. If necessary, specify the `HOST` and `PORT` environment variables to configure the listening interface and set the port number.

The converter is installed.

The Sigma rule converter is a plug-in for the pySigma framework, which means pySigma-backend-kuma can be used with other standard Sigma tools, not only a customized version of sigconverter.io. For example:

- sigma-cli is a converter with a command line interface.
- sigconverter.io is the original generic web interface.

README files for the libraries provided as source code:

- `src/pySigma/README.md` for the industry-standard sigma conversion framework and library.
- `src/pySigma-backend-kuma/README.md` for the plug-in for pySigma that implements KUMA filter and query conversion.
- `src/sigconverter.io/README.md` for the web interface.

After installation, log in to the web interface of the converter.

2. Adapt the correlation rule as necessary in the Sigma rule converter and copy or import the adapted rule into KUMA.

3. Restart the correlator to apply the changes.

Your adapted correlation is applied in the correlator.

Converting and uploading Sigma rules

To convert a Sigma rule to a KUMA rule:

1. Before adapting the rule, make sure that the following requirements are satisfied:

   - The predefined normalizers use event enrichment `to lower case` for fields containing user names, host names, and process names, therefore we recommend converting the relevant fields to lower case in the source Sigma rule.
   - We do not recommend adding `comments` or additional information to 'contains' conditions and other string validation conditions. If you do need to add a comment, use the # character. A comment does not affect a condition.
   - The rule must begin with the word `title` without hyphens before it.

2. Copy the correlation rule that you want to edit from the KUMA web interface, convert it to YML format, and paste it into the **rule.yml** tab of the converter. Select the settings in the drop-down lists as necessary. If you find errors during the check, fix the the errors.

3. In the Sigma rule converter, in the **Backend** field, select **kuma**, in the **Format** field, select **default**, and leave the **Pipeline** field empty.

   The following values are available:

   - Backend: kuma, Format: default—ready-to-run SQL query without formatting.
   - Backend: kuma, format: SQL_formatted—ready-to-run SQL query with formatting.
   - Backend: kuma_filter, Format: default—ready-to-use selector for the correlation rule.
   - Backend: kuma_filter, Format: correlation—ready-to-import correlation rule in JSON format. To perform the import, you can use the REST API method /api/v3/resources/correlationRule/create and specify the tenantID and the name of the tenant for the import.

4. Go to the tab of the **custom_pipeline.yml** converter and copy the example dictionary adapted for pySigma to that tab.

   Example dictionary adapted for pySigma

   Windows process_creation mapping

   product: windows

   category: process_creation

   DeviceEventClassID = 4688

   Windows sysmon EVENT=11 mapping

   product: windows

   service: Sysmon

   EventID = 11

   Windows security

   product: windows

   service: security

   EventID = 4624|4662|4104|4698

```
name: KUMA windows
priority: 30
transformations:
### Windows process_creation mapping

  - id: MAPPING_logsource_windows_process_creation
    type: field_name_mapping
    mapping:
      ParentImage: SourceProcessName
      Image: DestinationProcessName
      CommandLine: DeviceCustomString4
    rule_conditions:
```

```
      - type: logsource
        product: windows
        category: process_creation

  - id: DEFAULT_FOR_logsource_windows_process_creation
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
      DeviceEventClassID: '4688'
    rule_conditions:
       - type: logsource
         product: windows
         category: process_creation

### Windows sysmon EventID=11 mapping
  - id: DEFAULT_FOR_logsource_windows_sysmon
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Sysmon
    rule_conditions:
       - type: logsource
         product: windows
         service: Sysmon

  - id: MAPPING_logsource_windows_sysmon
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Image: OldFilePath
      CommandLine: DeviceCustomString4
      TargetFilename: FilePath
    rule_conditions:
      - type: logsource
        product: windows
        service: Sysmon

### Windows security mapping
  - id: DEFAULT_FOR_logsource_windows_security
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: DEFAULT_MAPPING_FOR_logsource_windows_security
    type: field_name_mapping
    mapping:
      Computer: DestinationHostName
      LogonID: FlexString1
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: 4624_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      LogonType: DeviceCustomNumber1
      SourceIP: SourceAddress
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4624

  - id: 4662_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Properties: FilePermission
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4662

  - id: 4104_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
```

```
    mapping:
      EventID: DeviceEventClassID
      ScriptBlockText: Message
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4104

  - id: 4698_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      TaskName: SourceProcessName
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: '4698'
```

The rule conversion result is displayed on the **query** tab. Depending on the scenario, the obtained result can be used as follows:

- As an SQL statement in a KUMA query
- As a filter in a KUMA correlation rule
- Imported into KUMA in JSON format as a correlation rule one by one.

Examples of supported Sigma rule conversions

Examples of supported Sigma rule conversions

Sigma rule	Mapping to KUMA objects	
title: Generic-DCSync Execution id: 9107f781-c984-436a-8093-1aaa64c70c49 description: Detects access to DC with "DS-Replication-Get-Changes" or "DS-Replication-Get-Changes-All" rights author: Kaspersky status: stable modified: 2023-08-02 tags: - attack.credential_access - attack.t1003.006 logsource: product: windows service: security detection: selection1: EventID: 4662 Properties|contains: - 'DS-Replication-Get-Changes' - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' selection2: EventID: 4624 LogonType: 3 filter: EventID: 4624 LogonType: 3 SourceIP: - '<ip address of DC servers>' timeframe: 1m condition: selection1 or (selection2 and not filter) | count(EventID) by Computer,LogonID = 2 fields: - SourceIP - Computer - LogonID - Username - Properties falsepositives: - Unknown level: high	"Microsoft products" normalizer tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows selection1: DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '' selection2 DeviceEventClassID=4624 DeviceCustomNumber1 = 3 filter DeviceEventClassID=4624 DeviceCustomNumber1 = 3 SourceAddress = <IP> condition: DeviceVendor = Microsoft AND DeviceProduct = Windows AND ((DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '') OR ((DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3) NOT (DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3 AND SourceAddress = <IP>))) everything inside Count() Pass EventID to Unique fields, everything after 'by' Computer → DestinationHostName LogonID → FlexString1 pass to Aggregation fields, everything after '=' or '>' pass 2 to threshold. timeframe pass to time window	Sigma correlation remove the pipe o converted into a c SQL query for Thr

Sigma rule	Mapping to KUMA objects	
title: Lsass Dump via LOLBin id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02 description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe references: - https://twitter.com/bohops/status/1635288066909966338 - https://twitter.com/mrd0x/status/1511415432888131586 modified: 2023-07-18 author: Kaspersky status: stable tags: - attack.credential_access - attack.t1003.001 logsource: product: windows category: process_creation detection: selection_procdump: Image|endswith: - '\procdump.exe' - '\procdump64.exe' CommandLine|contains: 'lsass' selection_dotnet: Image|endswith: '\dotnet-dump.exe' CommandLine: ' collect ' selection_dumpminitool: Image|endswith: '\dumpminitool.exe' condition: 1 of selection* falsepositives: - Unknown level: high	Converted in the same way as the rule in row 3 of the table. The difference is: the `condition` uses a `1 of selection` construct, where `selection` denotes one of the named groups of conditions.	DeviceVendor=' DeviceProduct= DeviceEventCla (((Desti '\\procdump.ex '\\procdump64. 'lsass') OR (Destinati dump.exe' AND De) OR Destinati '\\dumpminitoo)
title: Generic-Clearing Windows Event Logs via Command Line id: a903492e-da40-4ab4-a92d-306a4799d973 description: Detects Clear Windows Event Logs via Command Line author: Kaspersky status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1070.001 logsource: product: windows category: process_creation detection: selection1: Image|endswith: '\wevtutil.exe' CommandLine|contains: - ' cl ' - 'clear' selection2: Image|endswith: - '\powershell.exe' - '\powershell_ise.exe' - '\pwsh.exe' CommandLine|contains: - 'Clear-EventLog' - 'Remove-EventLog' selection3: Image|endswith: '\wmic.exe' CommandLine|contains: - 'ClearEventLog' condition: 1 of them falsepositives: - Legitimate System Administrator actions level: high	"Microsoft products" normalizer tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows DeviceEventClassID=4688 selection1: DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" Selection2 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" selection3 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" condition DeviceVendor = Microsoft AND DeviceProduct = Windows AND DeviceEventClassID=4688 AND ((DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains ""))) identical fields — specify the fields from the condition, except Name, deviceProduct, deviceVendor	DeviceVendor=' DeviceProduct= DeviceEventCla ((Destinati '\\wevtutil.ex (Devic DeviceCustomSt) OR ((Destin '\\powershell. Des '\\powershell\ '\\pwsh.exe') , (Device EventLog' OR D 'Remove-EventL) OR (Destinatio AND DeviceC 'ClearEventLog)

Sigma rule	Mapping to KUMA objects	
title: 0021-0002.1204.003 Execution - PowerExchangeDropper description: Detect the dropping of PowerExchange components. status: experimental logsource: product: windows service: Sysmon detection: selection1: EventID: 11 selection2: TargetFilename|contains: - 'c:\users\public\microsoftedge\autosave.exe' - 'c:\users\public\microsoftedge\wsdl.ps1' selection3: Image|endswith: "brochure.exe" condition: selection1 and selection2 and selection3 falsepositives: - Unknown level: high	Based on: Normalizer 11 of Sysmon event. title → name author → description description→ description status → description logsource DeviceVendor = Microsoft DeviceProduct = Sysmon selection1 DeviceEventClassID=11 selection2 FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '' if the file path contains * format in regexp selection3 OldFilePath endswith "" condition: DeviceVendor = Microsoft AND DeviceProduct = Sysmon AND (DeviceEventClassID=11) AND (FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '') AND (OldFilePath endswith "") identical fields — specify the fields from the condition, except Name, deviceProduct, deviceVendor level →severity falsepositive → Description	DeviceVendor=' DeviceProduct= DeviceEventCla (FilePath con 'c:\\users\\pu OR FilePath c 'c:\\users\\pu) AND OldFilePath en
title: Domain joined host discovery description: Detect an attacker enumerating domain-joined machines using PowerShell. status: stable logsource: product: windows service: security detection: selection: EventID: 4104 ScriptBlockText|contains|all: - 'System.DirectoryServices.DirectorySearcher' - 'Properties.operatingsystem' condition: selection falsepositives: - "Administrative scripts or tools like Vulnerability Scanners" level: medium	ScriptBlockText → Message	

Sigma rule	Mapping to KUMA objects	
title: 0022-0002.1053.005 Execution - PowerExchange Task description: Detect the creation of a scheduled task by PowerExchange. status: experimental logsource: product: windows service: security detection: selection: EventID: - '4698' TaskName|contains: - 'MicrosoftEdgeUpdateService' condition: selection falsepositives: - Unknown level: medium	TaskName → SourceProcessName	

Sigma rule	Mapping to KUMA objects	
title: Created Windows Shell from Critical Windows Process description: Anomaly behavior critical windows process status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1036 logsource: product: windows category: process_creation detection: selection: ParentImage|endswith: - '\searchindexer.exe' - '\lsaiso.exe' - '\lsm.exe' - '\spoolsv.exe' - '\wininit.exe' - '\smss.exe' - '\csrss.exe' - '\lsass.exe' - '\services.exe' - '\winlogon.exe' Image|endswith: - '\powershell_ise.exe' - '\cmstp.exe' - '\appvlp.exe' - '\mftrace.exe' - '\scriptrunner.exe' - '\forfiles.exe' - '\msiexec.exe' - '\rundll32.exe' - '\mshta.exe' - '\hh.exe' - '\wmic.exe' - '\regsvr32.exe' - '\scrcons.exe' - '\bash.exe' - '\sh.exe' - '\cscript.exe' - '\wscript.exe' - '\powershell.exe' - '\cmd.exe' condition: selection falsepositives: - Unknown level: high	ParentImage → SourceProcessName	

Segmentation rules

In KUMA, you can configure *alert segmentation rules*, that is, the rules for dividing similar correlation events into different alerts.

By default, if a correlation rule is triggered several times in the correlator, all correlation events created as a result of the rule triggering are attached to the same alert. Alert segmentation rules allow you to define the conditions under which different alerts are created based on the correlation events of the same type. This can be useful, for example, to divide the stream of correlation events by the number of events or to combine several events having an important distinguishing feature into a separate alert.

Alert segmentation is configured in two stages:

1. *Segmentation rules* are created. They define the conditions for dividing the stream of correlation events.

2. Segmentation rules are linked to the correlation rules within which they must be triggered.

Creating a segmentation rule

Alert segmentation rules are used to divide correlation events of the same type among different alerts. Conditions for correlation events for which separate alerts must be generated are specified in the segmentation rules.

To create a segmentation rule:

1. In the KUMA web interface, go to **Resources** → **Segmentation rules**, select a tenant and click the **Create new** button.

   This opens the **Create segmentation rule** window.

2. In the **Name** field, enter a name for the segmentation rule. The name must be unique and contain 1 to 128 Unicode characters.

3. If necessary, in the **Tenant** drop-down list, change the tenant to which the segmentation rule belongs.

4. In the **Type** drop-down list, specify the type of the segmentation rule. Available values:

   - **By filter**—an alert is created if the correlation events match the filter conditions specified in the **Filter** group of settings.

     You can use the **Add condition** button to add a string containing fields for identifying the condition. You can use the **Add group** button to add a group of filters. Group operators can be switched between **AND**, **OR**, and **NOT**. You can add other condition groups and individual conditions to filter groups. You can swap conditions and condition groups by dragging them by the ⠿ icon; you can also delete them using the ✕ icon. You can use operands and operators to specify conditions:

     - Left operand and Right operand—used to specify the values to be processed by the operator.

       The left operand contains the names of the event fields that are processed by the filter.

       For the right-hand operand, you can select the type of the value: **constant** or **list**, and specify the value.

     - **Available operators**

       - **=**—the left operand equals the right operand.

       - **<** means the left operand is less than the right operand.

       - **<=** means the left operand is less than or equal to the right operand.

       - **>** means the left operand is greater than the right operand.

       - **>=** means the left operand is greater than or equal to the right operand.

- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.

You can also add a filter in code mode. To do this, go to the **Code** tab in the **Filter** section and specify the filter in the input field. When entering parameter values, autocompletion is supported in the form of a list of hints. To display the list of all hints in the field, press **`Ctrl`**+**`Space`**.

> Note that the code mode allows you to use all possible values for rules in KUMA in the list of hints. Some of these values may not be valid for segmentation rules (for example, `activelist`, `dictionary`, `hasbit`).

- **By identical fields**—an alert is created if the correlation event contains the event fields specified in the **Correlation rule identical fields** drop-down list.

  You can select identical fields from the **Correlation rule identical fields** field by selecting check boxes. You can remove added fields by clicking the X icon next to the name of the identical field.

  If you have selected multiple event fields, an alert is generated if at least one of the selected fields is filled in the correlation event. Note that a separate alert is generated for each unique combination of correlation event fields. For example, if you have selected three fields: field 1, field 2, and field 3, the following alert creation options are possible:

  - Field 2 is filled, fields 1 and 3 are empty: alert 1 is created.
  - Field 2 is filled, fields 1 and 3 are empty. If the value of field 2 is the same as the value of field 2 in alert 1, a correlation event is added to alert 1. If the values of field 2 do not match, then alert 2 is created.
  - Field 3 is filled, fields 1 and 2 are empty: alert 3 is created.
  - Fields 2 and 3 are filled, field 1 is empty: alert 4 is created even if the value of field 2 is the same as the value of field 2 in alert 1, and the value of field 3 is the same as the value of field 3 in alert 3.
  - Fields 1, 2, and 3 are filled: alert 5 is created.

  Example of grouping fields usage

  A rule that detects a network scan generates only one alert, even if there are multiple devices that scan the network. If you create an alert segmentation rule based on the `SourceAddress` event grouping field and then bind this segmentation rule to a correlation rule, alerts are created for each address from which a scan is performed when the rule is triggered.

In this example, if the correlation rule name is "`Network. Possible port scan`", and the "`from {{.SourceAddress}}`" value is specified as the alert naming template in the segmentation rule resource, alerts are created that look like this:

- `Network. Possible port scan (from 10.20.20.20)`
- `Network. Possible port scan (from 10.10.10.10)`

- **By event limit**—an alert is created if the number of correlation events in the previous alert exceeds the value specified in the **Correlation events limit** field.

5. In the **Alert naming template** field, specify the template to be used for naming alerts generated by this segmentation rule. The default value is `{{.Timestamp}}`. In the template field, you can specify text, as well as event fields in the `{{.<Event field name>}}` format. When generating the alert name, the value of the event field is substituted instead of the event field name. The name of the alert created using the segmentation rules has the following format: `< Name of the correlation rule that created the alert > < text from the alert naming template field > < value of the specified event field >`. For example, if the triggered correlation rule name is named "`Connection. Insecure port usage`", and the segmentation rule name template contains `{{.Timestamp}}`, alerts of the following form are created:

   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:56:43 UTC)`
   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:59:46 UTC)`

   If multiple segmentation rules are executed with different alert naming templates, they are listed in the alert name separated by the `"|"` character.

6. If necessary, in the **Tags** drop-down list, select the tags for the event segmentation rule.

7. If necessary, enter a description of the segmentation rule in the **Description** field. You can enter up to 4,000 Unicode characters.

The segmentation rule is created. Next, you need to link the segmentation rule to a correlation rule.

Linking segmentation rules to correlation rules

Links between a segmentation rule and correlation rules are created for each tenant individually. They are displayed in the **Settings** → **Alerts** → **Segmentation** section of the KUMA web interface in the table with the following columns:

- **Tenant**—the name of the tenant that owns the segmentation rules.
- **Updated**—date and time of the last update of the segmentation rules.
- **Disabled**—this column displays a label if the segmentation rules are turned off.

To link an alert segmentation rule to the correlation rules:

1. In the KUMA web interface, open the **Settings** → **Alerts** → **Segmentation** section.

2. Select the tenant for which you would like to create a segmentation rule:

   - If the tenant already has segmentation rules, select it in the table.

   - If the tenant has no segmentation rules, click **Add settings for a new tenant** and select the relevant tenant from the **Tenant** drop-down list.

   A table with the created links between segmentation and correlation rule is displayed.

3. In the **Segmentation rule links** group of settings, click **Add** and specify the segmentation rule settings:

   - **Name** (required)—specify the segmentation rule name in this field. Must contain 1 to 128 Unicode characters.

   - **Tenants and correlation rules** (required)—in this drop-down list, select the tenant and its correlation rule to separate the events of this tenant into an individual alert. You can select several correlation rules.

   - **Segmentation rule** (required)—in this group of settings, select a previously created segmentation rule that defines the segmentation conditions.

   - **Disabled**—select this check box to disable the segmentation rule link.

4. Click **Save**.

   The segmentation rule is linked to the correlation rules. Correlation events created by the specified correlation rules are combined into a separate alert with the name defined in the segmentation rule.

To disable links between segmentation rules and correlation rules for a tenant:

1. Open the **Settings** → **Alerts** section of the KUMA web interface and select the tenant whose segmentation rules you want to disable.

2. Select the **Disabled** check box.

3. Click **Save**.

   Links between segmentation rules and correlation rules are disabled for the selected tenant.

Active lists

The *active list* is a bucket for data that is used by KUMA correlators for analyzing events according to the correlation rules.

For example, for a list of IP addresses with a bad reputation, you can:

1. Create a correlation rule of the operational type and add these IP addresses to the active list.

2. Create a correlation rule of the standard type and specify the active list as filtering criteria.

3. Create a correlator with this rule.

   In this case, KUMA selects all events that contain the IP addresses in the active list and creates a correlation event.

You can fill active lists automatically using correlation rules of the simple type or import a file that contains data for the active list.

You can add, copy, or delete active lists.

You can use active lists in correlation rules and dashboards.

The same active list can be used by different correlators. However, a separate entity of the active list is created for each correlator. Therefore, the contents of the active lists used by different correlators differ even if the active lists have the same names and IDs. The active list must be linked to a correlation rule, and the correlation rule must be linked to a correlator.

Only data based on correlation rules of the correlator are added to the active list.

You can add, edit, duplicate, delete, and export records in the active correlator sheet.

> If the correlator is disabled while processing active list data, the "Internal communication failed" error is displayed in the interface, indicating that the connection to the data source, namely the correlator, has been lost.

During the correlation process, when entries are deleted from active lists after their lifetime expires, service events are generated in the correlators. These events only exist in the correlators, and they are not redirected to other destinations. Correlation rules can be configured to track these events so that they can be processed and used to identify threats. Service event fields for deleting an entry from the active list are described below.

Event field	Value or comment
`ID`	Event identifier
`Timestamp`	Time when the expired entry was deleted
`Name`	`active list record expired`
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`ServiceID`	Correlator ID
`ServiceName`	Correlator name
`DeviceExternalID`	Active list ID
`DevicePayloadID`	Expired entry key
`BaseEventCount`	Number of deleted entry updates increased by one
S.<active list field>	Dropped-out entry of the active list in the following format: S.<active list field> = <value of active list field>

Viewing the table of correlator active lists

To view the table of correlator active lists:

1. In the KUMA web interface, select **Resources** → **Work with services** → **Active services**.
2. Select the check box next to the correlator for which you want to view the active list.
3. In the toolbar or in the menu (⋮), click **Go to active lists**.

   The **Correlator active lists** table is displayed.

Description of the Correlator active lists table

Column name	Description
Name	Active list name.
Records	The number of records in the active list.
Size on disk	Disk space occupied by the active list, KB.
Directory	Path to the active list on the KUMA Core server.

Adding active list

To add active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists.
2. In the KUMA web interface, select the **Resources** → **Resources** → **Active lists** section.
3. In the toolbar or in the menu (⋮), click **Add active list**.
4. Do the following:

   a. In the **Name** field, enter a name for the active list.

   b. In the **Tenant** drop-down list, select the tenant that owns the resource.

   c. In the **TTL** field, specify time in seconds for which the entry added to the active list must remain in it.

      When the specified time expires, the record is deleted. The time is specified in seconds.

      The default value is 0. If the value of the field is 0, the record is retained for 36,000 days (approximately 100 years).

   d. If necessary, in the **Tags** field, specify the tags to help find the resource.

   e. If necessary, enter additional information in the **Description** field.

      You can use up to 4,000 Unicode characters.

5. To save the active list, do one of the following:

   - Click the **Save** button.

   - Click the **Save with comment** button.

     If necessary, add a comment in the **Leave a comment** window that is displayed. To view comments for an active list, in the table of active lists, select the check box next to an active list and in the toolbar or in the menu (⋮) click **View versions history**. This opens the **Version history** window with a table of available versions of the active list, in which you can view comments.

The active list is added.

Viewing the settings of an active list

To view the settings of an active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists.

2. In the KUMA web interface, select **Resources** → **Resources** → **Active lists**.

   A table of available active lists is displayed.

3. In the **Name** column, select the active list whose settings you want to view.

The settings of the active list are displayed. For a description of active list settings, see the following table.

Settings of an active list

Setting name	Description
ID	Active list ID.
Name	Unique name of the active list
Tenant	Name of the tenant that owns the active list
TTL	Retention period of a record added to the active list. This value is specified in seconds.
Tags	Search tags of the active list
Description	Any additional information about the active list
Correlator	Name of the correlator to which the active list is linked. This field is displayed if the active list is linked to a correlator.

If the active list is linked to a correlator, the table of values of the active list is displayed.

Changing the settings of an active list

To change the settings of an active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists.

2. In the KUMA web interface, select **Resources** → **Resources** → **Active lists**.

   A table of available active lists is displayed.

3. In the **Name** column, select the active list whose settings you want to change.

4. Make the necessary changes to the following parameters:

   - **Name**—unique name of the active list
   - **TTL**—time to live parameter of entries stored in the Active list, in seconds.

     If the value of the field is 0, the record is retained for 36,000 days (approximately 100 years).
   - **Tags**—Search tags of the active list
   - **Description**—any additional information about the active list

   The **ID**, **Tenant**, and **Correlator** fields are not editable.

Duplicating an active list

To copy an active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists.
2. In the KUMA web interface, select **Resources** → **Resources** → **Active lists**.
3. Select the check box next to the active lists you want to copy.
4. In the toolbar or in the menu (⋮), click **Duplicate**.
5. Specify the name of the list and the tenant to which you want to copy the active list. By default, the active list that you are duplicating gets a name in the <Active_list_name>-copy format , and it is duplicated in the tenant that you are currently managing.
6. To save the active list, do one of the following:

   - Click the **Save** button.
   - Click the **Save with comment** button.

     If necessary, add a comment in the **Leave a comment** window that is displayed. To view comments for an active list, in the table of active lists, select the check box next to an active list and in the toolbar or in the menu (⋮) click **View versions history**. This opens the **Version history** window with a table of available versions of the active list, in which you can view comments.

The active list is copied.

Deleting active lists

To delete active lists:

1. In the KUMA web interface, select the tenants in which you want to manage active lists.
2. In the KUMA web interface, select **Resources** → **Resources** → **Active lists**.
3. Select the check boxes next to the active lists you want to delete.

If you want to delete all active lists, select the check box next to the **Name** column and in the context menu, select one of the following options:

- **Select all**
- **Select everything on the page**

> At least one check box must be selected.

4. Click the **Delete** button.
5. In the confirmation window, click **Delete**.

   If there are any links to the selected active lists from other resources and services, such lists cannot be deleted. In this case, you must first unlink the active lists from the correlation rules and correlators.

The active lists are deleted.

Viewing records in the active list

To view the records in the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:
   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.
   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.
2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened. If the active list is linked to a correlator, the table of values of the active list is displayed.

Description of the table of active list records

Setting name	Description
Key	Name of the active list key. Multiple values can be specified using the | character.
Value	Value of the active list key. You can specify multiple key values separated by commas in JSON format.
Actions	Actions that can be performed with active list records. You can edit or delete records.
Record repetitions	Total number of times the record was mentioned in events and identical records were downloaded when importing active lists to KUMA.
Expires	Date and time when the record will be deleted. If the **TTL** field had the value of 0 when the active list was created, the records of this active list are retained for 36,000 days (approximately 100 years).
Updated	The time when the active list was last updated.

The page can display up to 64 active list records. If necessary, you can scroll the page to view more records.

Searching for records in the active list

To find a record in the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.

2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened.

3. In the **Search** field, enter the record key name or several characters from the name. You can also search by key value.

The table of records of the active list displays only the records with the value containing the entered characters.

Adding a record to an active list

To add a record to the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and select one of the following options:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.

2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened.

3. Then click the **Add** button.

4. Specify the values of the following parameters:

   a. In the **Key** field, enter the name of the record.

      You can specify several values separated by the | character.

   b. In the **Value** field, specify a value in JSON format. You can specify multiple values.

5. Click the **Save** button.

   The record is added. After saving, the records in the active list are sorted in alphabet order.

The page can display up to 64 active list records. If necessary, you can scroll the page to view more items.

Duplicating records in the active list

To duplicate a record in the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.

2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened.

3. Select the check box next to the record that you want to copy.

4. Click **Duplicate**.

5. Specify the key and, if necessary, change the values of the key.

6. Click the **Save** button.

   The record is copied. After saving, the records in the active list are sorted in alphabet order.

The page can display up to 64 active list records. If necessary, you can scroll the page to view more items.

Changing a record in the active list

To edit a record in the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.

2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened.

3. Click the pencil icon in the **Actions** column.

4. Edit key values in JSON format.

5. If you want to confirm your changes, click the check mark in the **Actions** column. If you want to discard your changes, click the X mark in the **Actions** column.

6. Click **Save**.

   The record is overwritten. After saving, the records in the active list are sorted in alphabet order.

The page can display up to 64 active list records. If necessary, you can scroll the page to view more items.

Deleting records from the active list

To delete records from the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     The **Correlator active lists** table is displayed.

2. In the **Name** column, select the desired active list.

   A table of records for the selected active list is opened.

3. Select the check boxes next to the records that you want to delete.

   To delete all records, select the check box next to the **Key** column.

   > At least one check box must be selected.

4. Click the **Delete** button.

5. Click **OK**.

   The records will be deleted.

The page can display up to 64 active list records. If necessary, you can scroll the page to view more items.

Import entries to an active list

To import records into an active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed. Click the name of an active list to open the **Edit active list** window, and in that window, in the **Content** section, select the check boxes next to the records that you want to import.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the menu (⋮), click **Go to active lists**.

     In the **Correlator active lists** table that is displayed, select the check box next to the active sheet that you need.

2. In the toolbar, click **Import**.

   The active list import window opens.

3. Click the **Add** button to open a file selection window and select the file that you want to import.

4. In the **Format** drop-down list select the format of the file:

   - **csv**
   - **tsv**
   - **internal**

5. Under **Key field**, enter the name of the column containing the keys of records of the active list specified in the file. This field is not available for the **internal** format.

6. Click the **Import** button.

The data from the file is imported into the active list. The records included in the list before are saved.

Data imported from a file is not checked for invalid characters. If you use this data in widgets, widgets are displayed incorrectly if invalid characters are present in the data.

Exporting records from the active list

To export records from the active list:

1. In the KUMA web interface, select the tenants in which you want to manage active lists and do one of the following:

   - Go to the **Resources** → **Resources** → **Active lists** section.

     A table of available active lists is displayed. Click the name of an active list to open the **Edit active list** window, and in that window, in the **Content** section, select the check boxes next to the records that you want to export.

   - Go to the **Resources** → **Work with services** → **Active services** section.

     Select the check box next to the correlator for which you want to view the active list.

     In the toolbar or in the ⋮ menu, click **Go to active lists**.

     In the **Correlator active lists** table that is displayed, select the check box next to the active sheet that you need.

2. In the toolbar, click **Export**.

The active list is downloaded in JSON format to the default folder or to the folder specified in your browser settings. The name of the downloaded file reflects the name of active list.

Predefined active lists

The active lists listed in the table below are included in the KUMA distribution kit.

Predefined active lists

Active list name	Description
[OOTB][AD] End-users tech support accounts	This active list is used as a filter for the "[OOTB][AD] Successful authentication with same user account on multiple hosts" correlation rule. Accounts of technical support staff may be added to the active list. Records are not deleted from the active list.
[OOTB][AD] List of sensitive groups	This active list is used as a filter for the "[OOTB][AD] Membership of sensitive group was modified" correlation rule. Critical domain groups, whose membership must be monitored, can be added to the active list. Records are not deleted from the active list.
[OOTB][Linux] CompromisedHosts	This active list is populated by the [OOTB] Successful Bruteforce by potentially compromised Linux hosts rule. Records are removed from the list 24 hours after they are recorded.

Context tables

A *context table* is a container for a data array that is used by KUMA correlators for analyzing events in accordance with correlation rules. You can create context tables in the **Resources** section. The context table data is stored only in the correlator to which it was added using filters or actions in correlation rules.

You can populate context tables automatically using correlation rules of 'simple' and 'operational' types or import a file with data for the context table.

You can add, copy, and delete context tables, as well as edit their settings.

Context tables can be used in the following KUMA services and features:

- Correlation rules.
- Dashboard.

The same context table can be used in multiple correlators. However, a separate entity of the context table is created for each correlator. Therefore, the contents of the context tables used by different correlators are different even if the context tables have the same name and ID.

Only data based on correlation rules of the correlator are added to the context table.

You can add, edit, delete, import, and export records in the context table of the correlator.

> If the correlator is disabled while processing context table data, the "Internal communication failed" error is displayed in the interface, indicating that the connection to the data source, namely the correlator, has been lost.

When records are deleted from context tables after their lifetime expires, service events are generated in the correlators. These events only exist in the correlators, and they are not redirected to other destinations. Service events are sent for processing by correlation rules of that correlator which uses the context table. Correlation rules can be configured to track these events so that they can be used to process events and identify threats.

Service event fields for deleting an entry from a context table are described below.

Event field	Value or comment
`ID`	Event ID
`Timestamp`	Time when the expired entry was deleted
`Name`	`context table record expired`
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`ServiceID`	Correlator ID
`ServiceName`	Correlator name
`DeviceExternalID`	Context table ID
`DevicePayloadID`	Key of the expired entry
`BaseEventCount`	Number of updates for the deleted entry, incremented by one

`FileName`	Name of the context table.

`S.<context table field>`
`SA.<context table field>`
`N.<context table field>`
`NA.<context table field>`
`F.<context table field>`
`FA.<context table field>`
	Depending on the type of the entry that dropped out from the context table, the dropped-out context table entry is recorded in the corresponding type of event:
	for example, S.<context table field> = <context table field value>
	SA.<context table field> = <array of context table field values>
	
	Context table records of the boolean type have the following format:
	S.<context table field> = true/false
	SA.<context table field> = false,true,false

Viewing the list of context tables

You can view the full list of context tables or the list of context tables linked to a specific correlator.

Full list of context tables

To view the full list of context tables:

In the KUMA web interface, select **Resources** → **Resources** → **Context tables**.

The **Context tables** list is displayed.

List of context tables of a specific correlator

To view the context table list of the correlator:

1. In the KUMA web interface, select **Resources** → **Work with services** → **Active services**.
2. Select the check box next to the correlator for which you want to view the list of context tables.
3. In the toolbar or in the menu (⋮), click **Go to context tables**.

   The **Correlator context tables** list is displayed.

The table contains the following data:

- **Name**—name of the context table.
- **Records**—current number of records in the context table
- **Size on disk**—size of the context table.
- **Directory**—path to the context table on the KUMA correlator server.

Adding a context table

To add a context table:

1. In the KUMA web interface, select the **Resources** section.

2. In the **Resources** section, click **Context tables**.

3. In the **Context tables** window, click **Create new**.

   This opens the **Create context table** window.

4. In the **Name** field, enter a name for the context table.

5. In the **Tenant** drop-down list, select the tenant that owns the resource.

6. In the **TTL** field, specify time the record added to the context table is stored in it.

   When the specified time expires, the record is deleted. The time is specified in seconds. The maximum value is `31536000` (1 year).

   The default value is `0`. If the value of the field is 0, the record is stored indefinitely.

7. In the **Tags** drop-down list, select the tags for the context table that you are creating.

   The list includes all available tags created in the tenant of the resource and in the Shared tenant. You can find a tag in the list by typing its name in the field. If the tag you entered does not exist, you can press **`Enter`** or click **Add** to create it.

8. In the **Description** field, provide any additional information.

   You can use up to 4,000 Unicode characters.

   This field is optional.

9. On the **Schema** tab, specify which fields the context table has and the data types of the fields.

   Depending on the data type, a field may or may not be a key field. At least one field of the table must be a key field. All field names must be unique.

   To add a table row, click **Add** and fill in the table fields:

   a. In the **Name** field, enter the name of the field. The maximum length is 128 characters.

   b. In the **Type** drop-down list, select the data type for the field.

      Possible field data types

      Possible data types of context table fields

Field data type	Can be a key field	Comment
Integer	Yes	—
Float	Yes	—
String	Yes	—
Boolean	Yes	—
Timestamp	Yes	For a field of this type, it is checked that the field value is greater than or equal to zero. No other operations are provided.

Field data type	Can be a key field	Comment
IP address	Yes	For a field of this type, it is checked that the field value corresponds to the IPv4, IPv6 format. No other operations are provided.
Integer list	No	—
Float list	No	—
List of strings	No	—
Boolean list	No	—
Timestamp list	No	For a field of this type, it is checked that each item in the list is greater than or equal to zero. No other operations are provided.
IP list	No	For a field of this type, it is checked that each item of the list corresponds to the IPv4, IPv6 format. No other operations are provided.

c. If you want to make a field a key field, select the **Key field** check box.

A table can have multiple key fields. Key fields are chosen when the context table is created, uniquely identify a table entry and cannot be changed.

If a context table has multiple key fields, each table entry is uniquely identified by multiple fields (composite key).

10. Add the required number of context table rows.

After the context table is saved, changing the number of rows is not possible.

11. Then click the **Create** button.

The context table is added.

After adding the context table, link it to a correlation rule in the correlation rule settings in the **Context tables update** section. Then link this correlation rule to a correlator.

Once you linked the correlation rule to a correlator, the **Correlator** field and the **Content** section appear in the context table settings. From this section you can manage the context table contents.

Viewing context table settings

To view the context table settings:

1. In the KUMA web interface, select the **Resources** section.

2. In the **Resources** section, click **Context tables**.

3. In the list in the **Context tables** window, select the context table whose settings you want to view.

This opens the context table settings window. It displays the following information:

- **Name**—unique name of the resource.
- **Tenant**—the name of the tenant that owns the resource.
- **TTL**—the record added to the context table is stored in it for this duration. This value is specified in seconds.

- **Description**—any additional information about the resource.
- **Schema** is an ordered list of fields and their data types, with key fields marked.

Editing context table settings

To edit context table settings:

1. In the KUMA web interface, select the **Resources** section.
2. In the **Resources** section, click **Context tables**.
3. In the list in the **Context tables** window, select the context table whose settings you want to edit.
4. Specify the values of the following parameters:
   - **Name**—unique name of the resource.
   - **Tenant**—the tenant that owns the resource. This field is not editable.
   - **TTL**—the record added to the context table is stored in it for this duration. This value is specified in seconds.
   - **Tags** for resource search.
   - **Description**—any additional information about the resource.
   - **Correlator**—the correlator to which the correlation rule that uses the context table is linked. This field is not editable. This field appears after you link the correlation rule to a correlator.
   - **Content** is the content of the context table. This section appears after you link the correlation rule to a correlator.

     How to change the content of the context table

     To manually populate the context table or edit its content, you can:

     - Add, edit, or delete a row in the table
     - Duplicate a row

       Instead of creating a new row, you can select a row and duplicate it, edit the field values, and save.
     - Export the context table
     - Import the context table
5. Go to the **Schema** tab. This tab displays an ordered list of fields and their data types, with key fields marked. If the context table is not used in a correlation rule, you can edit the list of fields.

   If you want to edit the schema in a context table that is already being used in a correlation rule, follow the steps below.
6. Click **Save**.

To edit the settings of the context table previously used by the correlator:

1. Export data from the table.

2. Copy and save the path to the file with the data of the table on the disk of the correlator. This path is specified in the **Directory** column in the **Correlator context tables** window. You will need this path later to delete the file from the disk of the correlator.

3. Delete the context table from the correlator.

4. Edit context table settings as necessary.

5. Delete the file with data of the table on the disk of the correlator at the path from step 2.

6. To apply the changes (delete the table), update the configuration of the correlator: in the **Resources** → **Active services** section, in the list of services, select the check box next to the relevant correlator and click **Update configuration**.

7. Add the context table in which you edited the settings to the correlator.

8. To apply the changes (add a table), update the configuration of the correlator: in the **Resources** → **Active services** section, in the list of services, select the check box next to the relevant correlator and click **Update configuration**.

9. Adapt the fields in the exported table (see step 1) so that they match the fields of the table that you uploaded to the correlator at step 7.

10. Import the adapted data to the context table.

The configuration of the context table is updated.

Duplicating context table settings

To copy a context table:

1. In the KUMA web interface, select the **Resources** section.

2. In the **Resources** section, click **Context tables**.

3. Select the check box next to the context table that you want to copy.

4. Click **Duplicate**.

5. Specify the necessary settings.

6. Click the **Save** button.

The context table is copied.

Deleting a context table

> You can delete only those context tables that are not used in any of the correlators.

To delete a context table:

1. In the KUMA web interface, select the **Resources** section.
2. In the **Resources** section, click **Context tables**.
3. Select the check boxes next to the context tables that you want to delete.

   To delete all context tables, select the check box next to the **Name** column.

   > At least one check box must be selected.

4. Click the **Delete** button.
5. Click the **OK** button.

The context tables are deleted.

Viewing and finding records in the context table

To view a list of context table records:

1. Go to the full list of context tables or to the list of context tables of a specific correlator.
2. In the **Name** column, select the relevant context table.

   The list of records for the selected context table is displayed.

   To search the table, in the **Search** field, enter the value of a record key or the value of a field. The list of context table records displays only the records that contain the entered characters.

   If the your search query matches records with empty key values, the text <Nothing found> is displayed in the widget on the **Dashboard**. We recommend clarifying the conditions of your search query.

The list of records contains the following data:

- **Key** is the composite key of the record. It is comprised by one or more values of key fields, separated by the "|" character. If one of the key field values is absent, the separator character is still displayed.

  For example, a record key consists of three fields: `DestinationAddress`, `DestinationPort`, and `SourceUserName`. If the last two fields do not contain values, the record key is displayed as follows: `43.65.76.98| |`.

- **Record repetitions** is the total number of times the record was mentioned in events and identical records were downloaded when importing context tables to KUMA.

- **Expiration date** – date and time when the record must be deleted. The date and time format depends on the selected solution interface language.

  If the **Expires** field had the value of 0 when the context table was created, the records of this context table are retained for 36,000 days (approximately 100 years).

- **Updated**—date and time of the last update of the context table.

Adding, editing, and deleting records in the context table

To edit context table content:

1. Open the context table that you want to edit.

2. Do one of the following:

   - To add a row, click the **Add** button, then specify the field values and click the checkmark icon (✓) to save your changes. The fields indicated on the **Schema** tab as key fields must be filled.

     KUMA takes field names from the correlation rules with which the context table is associated. These names are not editable. The list of fields cannot be edited.

     If you do not specify some of the field values, the missing fields are populated with default values. The key of the record is determined from the full set of fields, and the record is added to the table. If an identical key already exists in the table, an error is displayed.

     List of default field values

Field type	Default value
Integer	0
Floating point number	0.0
String	""
Boolean	false
IP address	"0.0.0.0"
Timestamp	0
Integer list	[]
Float list	[]
List of strings	[]
Boolean list	[]
Timestamp list	[]
IP list	[]

   - To edit a row, in the **Actions** column, click the pencil icon (✎), then specify the field values and click the checkmark icon (✓) to save your changes.

     The value of the key field of the record is not available for editing. You can change it by exporting and importing a record.

     The values of the **Timestamp** and **Timestamp list** fields must be greater than or equal to 0. The values of the **IP address** and **IP address list** fields must conform to the IPv4 or IPv6 format.

- To duplicate a row, select a row and click the **Duplicate** button, then specify the field values and click the checkmark icon (✓) to save your changes.

- To delete a row, in the **Actions** column, click the trash can icon (🗑).

The context table is modified.

Exporting data from a context table

To export data from a context table:

1. In the KUMA web interface, select the **Resources** → **Active services** section.

2. Select the correlator whose context table you want to export, and in the toolbar or in the menu (⋮), click **Go to context tables**.

   This opens the **Correlator context tables** window.

3. Select the check box next to the context table that you want to export.

   You cannot export multiple context tables at the same time. Each table must be exported separately.

4. Click the **Export** button and select a format from the **Format** drop-down list:

   - **internal**

     The context table is exported in JSON format.

   - **csv**

   - **tsv**

5. Click the **Export** button.

   The context table is downloaded to your device in the selected format. The name of the exported file follows the following template: <context_table_name>_<export date (YYYY-MM-DD)>_<export time (HH-MM-SS)>. Exported data in the file is sorted by the **Key** field.

   When exporting in JSON (**internal**) format:

- The order of the fields in the file is not defined.

- Fields of the array type are exported to a file as an array of values, for example: `["val1","val2","val3","val4"]`.

- The date and time format in the **Timestamp** type field depends on the selected solution interface language.

When exporting in CSV and TSV formats:

- The first line of the file contains field names, and the subsequent lines contain the data.

- In the CSV format, the comma is used as a field separator, and in the TSV format, the tabulation character.

You can also export data into the context table in the context table settings window.

Importing data into a context table

To import data to a context table:

1. In the KUMA web interface, select the **Resources** section.
2. In the **Services** section, click the **Active services** button.
3. In the context menu of the correlator to whose context table you want to import data, select **Go to context tables**.

   This opens the **Correlator context tables** window.
4. Select the check box next to your context table and click **Import**.

   This opens the context table data import window.
5. Click **Add** and select the file that you want to import.
6. In the **Format** drop-down list select the format of the file:
   - **csv**
   - **tsv**
   - **internal**
7. Click the **Import** button.

The data from the file is imported into the context table. Records that previously existed in the context table are preserved.

When importing, KUMA checks the uniqueness of each record's key. If a record already exists, its fields are populated with new values obtained by merging the previous values with the field values of the imported record.

If no record existed in the context table, a new record is created.

> Data imported from a file is not checked for invalid characters. If you use this data in widgets, widgets are displayed incorrectly if invalid characters are present in the data.

You can also import data into the context table in the context table settings window.

Event enrichment

Event enrichment involves adding information to events that can be used to identify and investigate an incident.

Enrichment is performed using *enrichment rules*. Enrichment rules let you add supplementary information to event fields by transforming data that is already present in the fields, or by querying data from external systems. For example, suppose that a user name is recorded in the event. You can use an enrichment rule to add information about the department, position, and manager of this user to the event fields.

Enrichment rules can be used in collectors, correlators, and normalizers.

If you create enrichment rules in a collector or correlator, those enrichment rules are available for reuse. You can also link a separately created enrichment rule to a collector or correlator.

Enrichment rules created in the normalizer are linked only to the normalizer and are not available for reuse.

The solution comes with the following predefined enrichment rules:

- **[OOTB] Event categorization. Auditd** is an enrichment rule that allows to configure categorization for Auditd events.
- **[OOTB] Event categorization. Kaspersky Container Security** is an enrichment rule that allows to configure categorization for events received from Kaspersky Container Security.
- **[OOTB] Event categorization. Kaspersky Industrial CyberSecurity for Networks** is an enrichment rule that allows to configure categorization for events received from Kaspersky Industrial CyberSecurity for Networks.
- **[OOTB] Event categorization. Kaspersky IoT Secure Gateway** is an enrichment rule that allows to configure categorization for events received from Kaspersky IoT Secure Gateway.
- **[OOTB] Event categorization. Kaspersky Secure Mail Gateway** is an enrichment rule that allows to configure categorization for events received from Kaspersky Secure Mail Gateway.
- **[OOTB] Event categorization. Kaspersky Security Center** is an enrichment rule that allows to configure categorization for events received from Kaspersky Security Center.
- **[OOTB] Event categorization. Kaspersky Security for Linux Mail Server** is an enrichment rule that allows to configure categorization for events received from Kaspersky Security for Linux Mail Server.
- **[OOTB] Event categorization. Kaspersky Web Traffic Security** is an enrichment rule that allows to configure categorization for events received from Kaspersky Web Traffic Security.
- **[OOTB] Event categorization. Microsoft Products** is an enrichment rule that allows to configure the categorization for events from Microsoft products.
- **[OOTB] KATA alert** is a rule for enriching events received from Kaspersky Anti Targeted Attack Platform in the form of a hyperlink to an alert. The hyperlink is specified in the `DeviceExternalId` field.

  If you want the `DeviceExternalID` value to be displayed as a link in the event properties, make sure that the **Template** field in the rule properties for the `DeviceAddress` parameter contains a URL or fully qualified domain name followed by the `/` character, for example: `https://example.com:8443/` or `https://example.com/`.

Predefined enrichment rules can be deleted, but cannot be changed.

Viewing the enrichment rules

To view the enrichment rules:

1. In the web interface, go to **Resources** → **Enrichment rules**.

   Enrichment rules table opens.

You can use the **"Search"** field to search for enrichment rules. The search for enrichment rules is carried out using regular expressions.

You can sort the table by name, last update time, or package name by clicking the sort icon ⌄ in the column header and selecting either **Ascending** or **Descending**.

2. Click an enrichment rule to view its properties.

   This opens a window with the specified values of the enrichment rule. You can edit the enrichment rule as necessary.

Creating enrichment rule

To create an event enrichment rule:

1. In the web interface, go to one of the following sections:

   - **Resources** → **Enrichment rules**.
   - **Resources** → **List**

2. In the toolbar or menu ⋮, click the **Create** button.

3. In the sidebar that opens, enter a unique name for the enrichment rule in the **Name** field. The name must contain 1 to 128 Unicode characters.

4. In the **Tenant** drop-down list, select the tenant that will own this enrichment rule.

5. In the **Data source type** drop-down list, select the type of enrichment rule and configure the parameters specific to the selected data source type:

   constant

   This type of enrichment is used when a constant needs to be added to an event field. The settings of this type of enrichment are described in the table below.

   Parameters of enrichment type "constant"

Setting	Description
Constant	The value to be added to the event field. Maximum length of a value: up to 255 Unicode characters. If you leave this field blank, the existing event field value is removed.
Target field	The event field to insert the data into.

   If you are using the event enrichment functions for extended schema fields of `String`, `Number`, or `Float` type with a constant, the constant is added to the field.

   If you are using the event enrichment functions for extended schema fields of `Array of strings`, `Array of numbers`, or `Array of floats` type with a constant, the constant is added to the elements of the array.

   dictionary

   This type of enrichment is used if you need to add a value from the dictionary of the **Dictionary** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dictionary"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.

If you are using event enrichment with the **dictionary** type selected as the **Data source type**, and an array field is specified in the **Key enrichment fields** setting, then passing an array as a dictionary key will serialize the array into a string according to the rules of serializing a single value in TSV format.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`. The following values are passed to the dictionary as the key: `['a','b','c']`.

If the **Key enrichment fields** setting uses an extended schema array field and a regular event schema field, the field values are separated by the `|` character when the dictionary is queried.

Example. The **Key enrichment fields** setting uses the `SA.StringArrayOne` extended schema field and the `Code` string field. The `SA.StringArrayOne` extended schema field contains the values `"a"`, `"b"`, `"c"`, and the `Code` string field contains the `myCode` sequence of characters. The following values are passed to the dictionary as the key: `['a','b','c']|myCode`.

event

This type of enrichment is used when you need to write a value from another event field to the current event field. The settings of the enrichment type are described in the table below.

Parameters of enrichment type "event"

Setting	Description
Target field	The event field where the data needs to be inserted.
Source field	The event field whose value is written to the target field.
Conversion	The block of settings where you can create rules for modifying the original data before it is written to event fields. The conversion type can be selected from the drop-down list. You can use the **Add conversion** and **Delete** buttons to add or delete a conversion, respectively. The order of conversions is important.

Whether or not a conversion can be used depends on the type of an extended event schema field being used:

- For an additional field of the `String` type, all types of conversion are available.
- For the `Number` and `Float` type fields, the following types of conversion are available: **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String**, and **decodeBase64URLString**.
- For the `Array of strings`, `Array of numbers`, and `Array of floats` type fields, the following types of conversion are available: **append**, and **prepend**.

View available transformations

Conversions are modifications that are applied to a value before it is written to the event field.

You can select one of the following conversion types from the drop-down list:

- **entropy** is used for converting the value of the source field using the information entropy calculation function and placing the conversion result in the target field of the `float` type. The result of the conversion is a number. Calculating the information entropy allows detection of DNS tunnels or compromised passwords, for example, when a user enters a password instead of a login and the password gets logged in plain text.

- **lower**—is used to make all characters of the value lowercase

- **upper**—is used to make all characters of the value uppercase

- **regexp** – used to convert a value using a specified RE2 regular expression. When you select this type of conversion, a field is displayed in which you must specify the RE2 regular expression.

- **substring** is used to extract characters in a specified range of positions. When you select this type of conversion, the **Start** and **End** fields are displayed, in which you must specify the range of positions.

- **replace**—is used to replace specified character sequence with the other character sequence. When you select this type of conversion, the following fields are displayed:

  - **Replace chars** specifies the sequence of characters to be replaced.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- **trim** removes the specified characters from the beginning and from the end of the event field value. When you select this type of conversion, the **Chars** field is displayed in which you must specify the characters. For example, if it is necessary to execute a **trim** conversion with the value `Micromon` to `Microsoft-Windows-Sysmon`, the new value is `soft-Windows-Sys`.

- **append** appends the specified characters to the end of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **prepend** prepends the specified characters to the beginning of the event field value. When you select this type of conversion, the **Constant** field is displayed in which you must specify the characters.

- **replace with regexp** is used to replace RE2 regular expression results with the specified character sequence. When you select this type of conversion, the following fields are displayed:

  - **Expression** is the RE2 regular expression whose results you want to replace.

  - **With chars** is the character sequence to be used instead of the character sequence being replaced.

- Converting encoded strings to text:

  - **decodeHexString**—used to convert a HEX string to text.

  - **decodeBase64String**—used to convert a Base64 string to text.

  - **decodeBase64URLString**—used to convert a Base64url string to text.

  - **unicodeUnescape**—used to convert a Unicode string to text.

  When converting a corrupted string or if conversion error occur, corrupted data may be written to the event field.

During event enrichment, if the length of the encoded string exceeds the size of the field of the normalized event, the string is truncated and is not decoded.

If the length of the decoded string exceeds the size of the event field into which the decoded value is to be written, the string is truncated to fit the size of the event field.

We do not recommend using multiple extra normalizers for sequential conversion of the same field. The result of a conversion performed by an extra normalizer is not passed to the input of the next extra normalizer. The field in the resulting event contains the value produced by the extra normalizer that was the first to enrich this field.

- Converting the IP address to the IPv4 format:
  - **ipDecimalToDotted** converts an IP address in decimal format to an IP address in IPv4 format, in which octets are separated by dots.
  - **ipHexToDotted** converts an IP address in hexadecimal format to an IP address in IPv4 format, in which octets are separated by dots.
- **hexToDecimal** is used to convert a numeric value from hexadecimal notation to decimal. The conversion is applied to string or numeric fields containing HEX values (including the 0x prefix, if present), and the result is written to the target field of the KUMA event as an integer.

  The result of the conversion is a decimal number, for example, an initial value of 0x00FF is converted to 255.

template

This type of enrichment is used when you need to write a value obtained by processing Go templates into the event field. We recommend matching the value and the size of the field. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "template"

Setting	Description
Template	The Go template. Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field from which the value must be passed to the script, for example, `{{.DestinationAddress}} attacked from {{.SourceAddress}}`.
Target field	The event field to insert the data into.

If you are using enrichment of events that have **template** selected as the template, and in which the target field has the `String` type, and the source field is an extended event schema field containing an array of strings, you can use one of the following examples for the template:

- `{{.SA.StringArrayOne}}`
- `{{- range $index, $element := . SA.StringArrayOne -}}`
  `{{- if $index}}, {{end}}"{{$element}}"{{- end -}}`

To convert the data in an array field in a template into TSV format, use the `toString` function, for example:

```
template {{toString.SA.StringArray}}
```

table

This type of enrichment is used if you need to add a value from the dictionary of the **Table** type. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "table"

Setting	Description
Dictionary name	The dictionary from which the values are to be taken.
Key fields	Event fields whose values are to be used for selecting a dictionary entry. To add an event field, click **Add field**. You can add multiple event fields.
Mapping	Event fields for data transfer: • **Dictionary field** specifies dictionary fields from which data is to be transmitted. The available fields depend on the selected dictionary resource. • **KUMA field** specifies event fields to which data is to be transmitted. In the **Label** column, you can assign a name to the written data for the selected fields (`*custom*` and `*flex*`).

The first field in the table (**Dictionary field**) is taken as the key with which the fields selected from the event as key fields are matched (**KUMA field**). As the key in the **Dictionary field**, you must select an indicator of compromise by which the enrichment is to be performed, for example, IP address, URL, or hash. In the rule, you must select the event field that corresponds to the selected indicator of compromise in the dictionary field.

If you want to select multiple key fields, you can specify them using `|` as a separator (when specifying in the web interface or importing as a CSV file), for example, `<IP address>|<user name>`.

You can add new table rows or delete table rows. To add a new table row, click **Add new element**. To delete a row in the table, click the ✕ cross.

enrichment by assets

You can use this type of enrichment when you need to add enrichment of events with assets to specific collectors.

To enrich events with assets in the **Mapping** block, fill in the mapping table of the KUMA event fields and the fields used to record values from the hash table.

To fill in the field mapping table:

1. In the **Matching** block, click **Add**.

2. In the **KUMA field** drop-down list, select one or more event fields that you want to map to values from the hash table and write to the corresponding field in the asset information table.

3. In the **Field to write data to** drop-down list, select the field into which the asset ID value will be written when the event field (**KUMA field**) matches the value from the hash table.

   Possible parameter values in the field mapping table

KUMA field	KUMA event field to write to

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

When you specify multiple fields, the **AND** operator is applied to field values. If you add multiple strings in the **KUMA field** column, the **OR** operator is applied to field values. The matching begins from the first field in the list. If the value of the field matches the value of the attribute, matching stops.

For example, suppose that the following data is received in an event:

`SourceAddress=192.168.x.xx`
`SourceHostName=kuma.example.com`

There are two assets in KUMA: `company.example.com` (IP address: `192.168.x.xx`; FQDN: `company.example.com`) and `kuma.example.com` (IP address: `192.168.y.yyy`; FQDN: `kuma.example.com`). Matching is performed as follows:

- If you specify `sourceAddress` → `sourceAssetID`, and then `sourceHostname` → `sourceAssetID` separately, then the asset will correspond to the first condition (`company.example.com`).
- If it is more important to get the `sourceHostname` parameter value (`kuma.example.com`), then `sourceHostname` → `sourceAssetID` must be specified first followed by `sourceAddress` → `sourceAssetID`.
- If you specify `sourceAddress` + `sourceHostname` → `sourceAssetID`, there will be no enrichment.

> At least one matching condition must be specified in the field mapping table.

4. To apply the default values for the **KUMA field** and **Field for data recording** parameters, click the button. **Apply the default mapping** located above the table.

   Default parameter values

KUMA field	KUMA event field to write to
`DestinationAddress`	`DestinationAssetID`
`DestinationHostName`	`DestinationAssetID`
`DeviceAddress`	`DeviceAssetID`
`DeviceHostName`	`DeviceAssetID`
`SourceAddress`	`SourceAssetID`
`SourceHostName`	`SourceAssetID`

dns

This type of enrichment is used to send requests to a private network DNS server to convert IP addresses into domain names or vice versa. IP addresses are converted to DNS names only for private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "dns"

Setting	Description
URL	URL of the DNS server to which you want to send requests. You can use the **Add URL** button to specify multiple URLs. If the **URL** setting is not specified, KUMA takes the list of DNS servers from the localhost's `/etc/resolv.conf` file. In this case, you need to enable the **Recursive queries** option. Otherwise, the enrichment will not occur.
Requests per second	Maximum number of queries sent to the DNS server per second. By default, this value is equal to the number of vCPUs of the KUMA Core server.

Setting	Description
Workers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used. The default value is `1`.
Maximum number of events in enrichment queue	The maximum number of events to hold in the resubmission queue. The default value is `1,000,000`.
Timeout	The time to wait for a response from the DNS server (in seconds). The default value is `5`.
DNS mode override	Resolution method used: • **Forward DNS only** resolves a domain name to an IP address. • **Reverse DNS only** resolves an IP address to a domain name. • **Forward and reverse DNS** resolves a domain name to an IP address or an IP address to a domain name.
Cache TTL	The lifetime (in seconds) of values stored in the cache. The default value is `60` seconds.
Cache disabled	You can enable or disable caching using this setting. Caching is enabled by default.
Cache refresh disabled	If cache update is enabled, then upon expiry of the cache's TTL the collector sends repeated requests to the DNS server to update the data stored in the cache. This setting is available only when cache is enabled. By default, cache update is enabled.
Recursive queries	Allows a collector to send recursive queries to authoritative DNS servers for the purposes of enrichment. The default value is **Disabled**.

cybertrace

For systems with high load on a collector or correlator, we recommend using the **cybertrace-http** enrichment type. This type of enrichment returns a structured JSON response and correctly distinguishes between strings and arrays of custom attributes, preventing parsing errors.
When **cybertrace** enrichment is used, the collector receives an unstructured response. If the value of a custom attribute in Kaspersky CyberTrace contains square brackets, for example, **[str1**, **str2]**, Kaspersky SIEM treats it as an array, not a string.

This type of enrichment is used to add information from Kaspersky CyberTrace data feeds to event fields. The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace"

Setting	Description
URL	URL of the Kaspersky CyberTrace server which you want to send requests to. The default Kaspersky CyberTrace port is 9999. Required setting.
Number of connections	Maximum number of connections to the Kaspersky CyberTrace server that can be established simultaneously by Kaspersky SIEM. By default, this value is equal to the number of vCPUs of the KUMA Core server.
Requests per second	Maximum number of requests sent to the server per second. The default value is `1000`.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`.
Mapping	Table for mapping event fields to the types of indicators in Kaspersky CyberTrace. The **KUMA field** column shows the names of event fields, and the **CyberTrace indicator** column shows the types of Kaspersky CyberTrace indicators. Available types of Kaspersky CyberTrace indicators: • **ip** • **url** • **hash**

In the mapping table, you must provide at least one string. You can add new table rows or delete table rows. To add a new table row, click **Add row**. To delete a row in the table, click the ✕ cross.

cybertrace-http

This streaming event enrichment type in Kaspersky CyberTrace allows you to send a large number of events to the CyberTrace API-interface with a single request. We recommend using the **cybertrace-http** enrichment type for systems with a large stream of events. The **cybertrace-http** enrichment type performs better than the **cybertrace** enrichment type.

Limitations:

- The **cybertrace-http** enrichment type cannot be used for retrospective scanning in KUMA.
- When the **cybertrace-http** enrichment type is used, cyberthreat detections are not saved in Kaspersky CyberTrace history in the **Detections** window.

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "cybertrace-http"

Setting	Description
Tenant	Tenant, within which you plan to work with Kaspersky CyberTrace. Required setting.
URL	URL of the Kaspersky CyberTrace server to which you want to send requests, and the port used by the CyberTrace API. The default port is 443. Required setting.
Secret	The drop-down list where you can select the secret that stores the connection credentials. Required setting.
Timeout	Timeout for a response from the Kaspersky CyberTrace server, in seconds. The default value is `30`.
Key fields	The list of event fields used for enriching events with data from Kaspersky CyberTrace. Required setting.
Maximum number of events in the enrichment queue	Maximum number of events that are stored in the enrichment queue. The default value is `1,000,000`. After reaching 1 million events received from the Kaspersky CyberTrace server, events stop being enriched until the number of received events is reduced to less than 500,000.
CyberTrace main version	Kaspersky CyberTrace version. Available values: • **<5**—requests are executed in the General tenant in Kaspersky CyberTrace, and use the new API version provided by Kaspersky CyberTrace 5.0 and later. • **≥ 5.0**—requests use the API version that corresponds to Kaspersky CyberTrace 4.x. The default value is **<5**.
Debug	The parameter that enables resource logging. The toggle switch is turned off by default.
Tags	Tags for resource search.

timezone

This type of enrichment is used in collectors and correlators to assign a specific time zone to an event. Time zone information may be useful when searching for events that occurred at unusual times, such as nighttime.

When this type of enrichment is selected, the required time zone must be selected from the **Time zone** drop-down list.

> Make sure that the selected time zone is set on the server hosting the enrichment-utilizing service. For example, you can do this by using the `timedatectl list-timezones` command, which shows all time zones that are set on the server. For more details on setting time zones, please refer to your operating system documentation.

When an event is enriched, the time offset of the selected time zone relative to Coordinated Universal Time (UTC) is written to the DeviceTimeZone event field in the `+-hh:mm` format. For example, if you select the **Asia/Yekaterinburg** time zone, the value `+05:00` will be written to the `DeviceTimeZone` field. If an enriched event already has a value in the `DeviceTimeZone` field, it will be overwritten.

By default, if the timezone is not specified in the event being processed and enrichment rules by timezone are not configured, the event is assigned the timezone of the server hosting the service (collector or correlator) that processes the event. If server time is changed, the service must be restarted.

Permissible time formats when enriching the DeviceTimeZone field

When processing incoming raw events in the collector, the following time formats can be automatically converted to the `+-hh:mm` format (see the table below):

Time format in a processed event	Example
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

If the date format in the `DeviceTimeZone` field differs from those listed in the table, the collector server time zone is written to the field when an event is enriched with time zone information. You can create normalization rules for non-standard time formats.

geographic data

This type of enrichment is used to add IP address geographic data to event fields.

When this type is selected under **Mapping geographic data to event fields** parameter block, you need to specify from which event field the IP address will be read, select the attributes of geographic data, and define the event fields to which geographic data will be written:

1. In the **Event field with IP address** drop-down list, select the event field from which the IP address is read. Geographic data uploaded to KUMA is matched against this IP address.

   > When the `SourceAddress`, `DestinationAddress`, and `DeviceAddress` event fields are selected, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields.

2. For each event field you need to read the IP address from, select the type of geographic data and the event field to which the geographic data should be written.

   - In the **Geodata attribute** field, select which geographic data corresponding to the read IP address should be written to the event. Available geographic data attributes: **Country**, **Region**, **City**, **Longitude**, **Latitude**.

   - In the **Event field to write to**, select the event field which the selected geographic data attribute must be written to.

   You can use the **Add geodata attribute** button to add field pairs for **Geodata attribute** – **Event field to write to**. You can also configure different types of geographic data for one IP address to be written to different event fields.

3. To add each subsequent mapping, click the **Add mapping** button and repeat the previous two steps of these instructions.

   You can write identical geographic data attributes to different event fields. If you configure multiple geographic data attributes to be written to the same event field, the event will be enriched with the last mapping in the sequence.

check DLL Hijacking

DLL Hijacking is an attack technique that involves delivering vulnerable legitimate software along with a malicious dynamic link library (DLL) to a target system. To detect such attacks, Kaspersky SIEM uses the AI module. The AI module analyzes the launch and runtime parameters of applications and identifies suspicious launches of legitimate software with malicious libraries.

To get a status, Kaspersky SIEM sends a request with information from event fields to <KSN>. In response to the request, KSN sends the analysis result.

You can configure DLL Hijacking attack detection in the collector or correlator.

> To use enrichment such as **check DLL Hijacking**, your license must include the AI module. The General administrator needs also to accept the additional KSN Statement in the **Kaspersky Security Network** section (**Settings** → **Integrations** → **AI services** → **DLL Hijacking detection**).

The settings of this type of enrichment are described in the table below.

Parameters of enrichment type "DLL Hijacking"

Setting	Description
Handlers	Number of handlers that the service can run simultaneously to process response rules in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.
Maximum cache size	Maximum cache size for KSN responses, in megabytes. The default value is `128 MB`. Each KSN response has its own lifetime, during which it is retained in the cache. If Kaspersky SIEM sends a second request for a DLL file for which KSN has already issued a response, and the lifetime of that response has not yet expired, the request is not actually sent to KSN, but the response is taken from the cache.
Maximum number of events in enrichment queue	If the specified value is exceeded, new events are not processed. The default value is `1,000,000`. `0` means that event processing stops if the queue contains any number of events.

Perform a repeat request	KSN response may return the **Unclassified** status. This status means that KSN has accepted the request and is currently processing it, but there is no status yet. Processing may take a long time, so the request must be re-sent.
	If this setting is enabled, specify additional settings:
	• If the **Create duplicates** setting is enabled, KUMA creates a duplicate event and uses it for repeated requests to KSN. In this case, the main event is routed in accordance with the workflow. A duplicate event is written to the database when one of the following conditions is satisfied:
	  • A status other than **Unclassified** is received from KSN.
	  • The disk buffer configured using the **Buffer size** setting is full.
	  • The **Request count** is exceeded.
	If this setting is disabled, KUMA continues to send requests using the main event. The event is written to the database when one of the following conditions is satisfied:
	• A status other than **Unclassified** is received from KSN.
	• The disk buffer configured using the **Buffer size** setting is full.
	• The **Request count** is exceeded.
	• The **Request count** is the maximum number of requests to KSN. If a status other than **Unclassified** is not received by executing the specified number of requests, the event is written to the database with the **Unclassified** status. The default value is `10`.
	• **Poll interval** is the interval between requests, in minutes. The default value is `1 minute`. The minimum value is `1 minute`.
	• **Buffer size** is the size of the disk buffer for events awaiting a repeat request, in megabytes. The default value is `10240 MB`. The minimum value is `10 MB`.

Proxy server	Proxy server settings, if one is needed to connect to the KSN server. You can select one of the available proxy servers or create a new proxy server. By default, a proxy server is not used.
Mapping	The table of parameters that must be sent in a KSN request to get a status, and a list of the corresponding KUMA event fields. • **DLL file hash (md5)**—a recommended mapping field: `OldFileHash`. • **DLL file path**—a full path including a file name. Recommended field for mapping: `OldFilePath`. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **Process hash (md5)**—a recommended mapping field: `FileHash`. • **process path**. Full path including the file name. Since the path may contain personal data, Kaspersky SIEM sends this parameter to KSN in an anonymized form. For example: Path before anonymization: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` The same path in anonymized form: `device\harddiskvolume1\users\username` • **DLL file name**—a recommended mapping field: `OldFileName`. • **Process name**—a recommended mapping field: `FileName`. • **Process signature** is a field that specifies the KUMA field that transfers the `Organization` from the signature `Subject`. If these values are not available, leave the signature empty. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** column, select **process signature** from the drop-down list (optional). Recommended field for mapping: FileID. • **dll size**. Optional; recommended field for mapping: OldFileSize. To add this parameter, click the **Add** button, then in the **DLL Hijacking field** field, select **dll size** from the drop-down list. For each parameter, specify a corresponding KUMA event field in the table.

6. If you want to enable logging of service operations, turn on the **Debug** toggle switch.

7. If necessary, in the **Tags** drop-down list, select thetags for the enrichment rule.

8. If required, add a description for the enrichment rule in the **Description** field. The rule description can contain up to 4000 Unicode characters.

9. If you want to specify conditions that define which events are processed by the enrichment rule, in the **Filter settings** section, select or create a filter from the **Filter** drop-down list.

   How to create a filter

   All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default.

To create a filter:

1. In the **Filter** drop-down list, select **Create new**.

2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default.

3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters.

4. Select the filter creation mode: **Constructor** or **Code**.

   When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code.

5. If you selected the **Constructor** option, do the following:

   a. In the drop-down list select a boolean operator:

      - **AND**: selects events that match all of the specified conditions.

      - **OR**: selects events that match one of the specified conditions.

      - **NOT**: selects events that match none of the specified conditions.

   b. Click the **Add condition** button.

   c. If you want to add a negative condition, from the **If** drop-down list, select **If not**.

   d. From the drop-down lists, select operands and filter operators.

      Operands of filters

      - **Event fields** specify the field of the event that you need to use as a filter operand.

      - **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**.

        If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand.

      - **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings:

        - **dictionary** (required) is the dictionary that you want to use.

        - **key fields** (required) are event fields that are used to generate the key of the dictionary value.

      - In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field:

        - **context table name** (required) is the context table that you want to use.

        - **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record.

- **field** is the name of the context table field from which you want to get the value of the operand.
- **index** is the index of the list field of the table from which you want to get the value of the operand.

- **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings:
  - **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type.
  - **key fields** (required) are event fields that are used to generate the key of the dictionary value.
- **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings:
  - **stream** (required) is the Kaspersky CyberTrace threat category.
  - **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators.
  - **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.
- **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
  - **value** (required) is the constant that you want to assign to the operand.
- **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
  - **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.

Filter operators

- **=** means the left operand equals the right operand.
- **<** means the left operand is less than the right operand.
- **<=** means the left operand is less than or equal to the right operand.
- **>** means the left operand is greater than the right operand.
- **>=** means the left operand is greater than or equal to the right operand.
- **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
- **contains** means the left operand contains values of the right operand.
- **startsWith** means the left operand starts with one of the values of the right operand.
- **endsWith** means the left operand ends with one of the values of the right operand.
- **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
- **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).

  The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.

If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.

- **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.

  If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.

- The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.

- **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.

- **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.

- **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.

- **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.

- **inContextTable** checks for the presence of the entry in the specified context table.

- **intersect** checks for the presence in the left operand of the list items specified in the right operand.

If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.

You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **`Backspace`**.

e. To add a group of conditions for the filter, click the **Add group** button.

   You can add multiple condition groups.

6. If you selected the **Code** option, specify the text filter command.

   In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.

7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.

8. Click **Save**.

10. Then click the **Create** button.

The enrichment rule is created and displayed in the table.

Linking the enrichment rules

To link an enrichment rule to a collector or correlator:

1. In the web interface, go to **Resources** → **Enrichment rules**.
   The enrichment rule table is displayed.
2. Select the check box next to one or more enrichment rules.
3. In the toolbar or menu ⋮, click **Link to service** and select one of the following options:
   - **Link to collector**.
   - **Link to correlator**.
4. In the panel that opens, select one or more correlators or collectors, and click **OK**.

The enrichment rule is linked to the selected services and is applied in accordance with their configuration.

You can remove the enrichment rule link from the collector or correlator when the rule is changed.

Managing enrichment rules

This article describes how to edit and duplicate an enrichment rule, how to view dependencies and versions, and how to delete a rule.

Changing an enrichment rule

To edit the enrichment rule:

1. In the web interface, go to one of the following sections:
   - **Resources** → **Enrichment rules**.
   - **Resources** → **List**
     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Enrichment rule**.
2. Click an enrichment rule that you want to edit.
   The **Edit enrichment rule** pane opens on the right.
3. Make necessary changes.

4. If you want to link an enrichment rule to a collector or correlator, or to remove this link, open the **Services** tab and do the following:

   - To link an enrichment rule, click **Link to service** and select **Link to collector** or **Link to correlator**. In the pane that opens, select one or more collectors or correlators and click **OK**.

   - To remove the link for the enrichment rule, select the check boxes next to the required collectors or correlators, click **Delete** and confirm the action.

5. Click **Save**.

   The enrichment rule is changed.

Creating an enrichment rule based on an existing one

To create a copy of an enrichment rule:

1. In the web interface, go to one of the following sections:

   - **Resources** → **Enrichment rules**.

   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Enrichment rule**.

2. Select the check box next to the enrichment rule that you want to copy.

3. In the toolbar or in the menu (⋮), click **Duplicate**.

4. In the **Create enrichment rule** pane that opens, specify the settings of the created rule.

5. Click **Save**.

   The enrichment rule is created based on the existing rule.

Viewing dependencies

For each enrichment rule, you can open a dependency graph.

To view dependencies:

1. In the web interface, go to one of the following sections:

   - **Resources** → **Enrichment rules**.

   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Enrichment rule**.

2. Select the check box next to the enrichment rule.

3. In the toolbar or in the menu (⋮), click **Show dependencies**.

   The enrichment rule dependencies window opens.

4. If you want to download the dependency data, click the **Download SVG** button.

5. If necessary, configure filters to display dependencies on the graph using the **Show on graph** drop-down list.

Viewing the version history

To view the version history of the enrichment rule:

1. In the web interface, go to one of the following sections:

   - **Resources** → **Enrichment rules**.

   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Enrichment rule**.

2. Select the check box next to the enrichment rule that you want to view.

3. In the toolbar or in the ⋮ menu, click **View versions history**.

4. If necessary, you can compare the versions with each other. To do this, select the check boxes next to the versions you want to compare and click **Compare**.

5. If you want to restore an earlier version of a rule, select the check box next to the name of this rule, click **Restore**, and then confirm the action.

Deleting an enrichment rule

To delete an enrichment rule:

1. In the web interface, go to one of the following sections:

   - **Resources** → **Enrichment rules**.

   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Enrichment rule**.

2. Select the check boxes next to enrichment rules that you want to delete.

3. In the toolbar or in the menu (⋮), click **Delete**.

4. Confirm the removal.

The enrichment rules are deleted.

Adding enrichment rules in collector properties

You can configure enrichment of events received by only those collectors for which you need it. To do this, add one or more enrichment rules in the properties of the collector.

To add enrichment rules in collector properties:

1. In the web interface, under **Resources** → **Collectors**, select the relevant tenant.

   The collectors table opens.

2. Click the name of the collector for which you want to add an enrichment rule.

3. In the sidebar that opens, select the **Event enrichment** section.

4. Click the **Add enrichment** button.

5. In the **Enrichment rule** drop-down list, select an enrichment rule.

   You can also create a collector enrichment rule by clicking **Create** in the **Enrichment rule** drop-down list.

6. If necessary, add another enrichment rule by clicking the **Add enrichment** button.

   > You cannot add the same enrichment rule more than once.

7. Click **Save**.

Kaspersky SIEM applies the added enrichment rule when the collector receives and processes messages from event sources.

Enriching events with assets

Many devices (assets) of various types can be connected to a company's corporate network, such as servers, workstations, laptops, mobile devices, and IoT devices. Assets are identified by properties such as IP address, FQDN, and MAC address. To ensure the security of a corporate network, you may need to:

- track assets and their properties during correlation and for conducting investigations;
- use assets and their properties to trigger correlation rules;
- track asset status using widgets and reports;
- maintain an up-to-date list of assets with unpatched vulnerabilities;
- monitor traffic from IoT devices, such as webcams, refrigerators, and coffee machines.

To address these issues, you can use event enrichment with assets.

Enriching events with assets involves the following steps:

1. **Adding assets to KUMA and defining their properties**

   This can be done in the following ways:

   - Import assets from:
     - Kaspersky Security Center Windows or Kaspersky Security Center Linux;
     - KICS for Networks or KATA;
     - MaxPatrol VM;
     - nmap report.
   - Add assets manually.
   - Add assets via REST API.

2. **Adding custom fields to asset properties**

   If the existing fields of the asset data model are not sufficient, you can create custom asset fields and then populate them in the asset properties manually or via the REST API.

   For example, if you want to categorize IoT devices by type, you can create a custom `IoT type` field. Then, in the **Assets** section of the KUMA web interface, find all IoT devices and specify the device type in the `IoT type` field in properties of each device, for example: `webcam`, `refrigerator`, `coffee machine`.

3. **Setting up asset categorization**

   You can group assets into categories, which you can then use to configure correlation rules. When creating categories, you can use asset properties as conditions for category assignment, such as the presence of vulnerabilities, the IoT device type, or antivirus database relevance. You can assign a severity to each category from low to critical.

4. **Configuring rules of enriching events with assets**

   Since asset enrichment increases the load on the collector service, it is recommended to choose on which collectors to configure asset enrichment. This can be done based on the type and function of event sources that send events to the collector. You can configure asset enrichment on all collectors and later disable it on collectors that do not require it.

   Event enrichment is configured in the **Event enrichment** step when creating a collector. To do this, you need to create and configure an enrichment rule of **the asset enrichment** type. You can do this either in the **Event enrichment** step or by creating an enrichment rule in advance and then linking it to the collector.

   The logic of the asset enrichment rule is as follows: When an event arrives at the collector, KUMA checks whether the `SourceAddress`, `DestinationAddress`, `DeviceAddress`, `SourceHostName`, `DestinationHostName`, and `DeviceHostName` fields are filled in. The IP address or FQDN values from these fields are then compared with the IP address and FQDN values from the properties of assets added to KUMA. Thus, matching values from the event fields and asset properties allows KUMA to determine which asset is specified in the event. Next, KUMA writes the `AssetID` value of the matched asset to one or more of the following event fields: `SourceAssetID`, `DestinationAssetID`, and `DeviceAssetID`. The events are then sent to a correlator or storage.

   For example, suppose that the following data is received in an event:

   ```
   SourceAddress=192.168.x.xx
   SourceHostName=kuma.example.com
   ```

There are two assets in KUMA: `company.example.com` (IP address: `192.168.x.xx`; FQDN: `company.example.com`) and `kuma.example.com` (IP address: `192.168.y.yyy`; FQDN: `kuma.example.com`). Matching is performed as follows:

- If you specify `sourceAddress` → `sourceAssetID`, and then `sourceHostname` → `sourceAssetID` separately, then the asset will correspond to the first condition (`company.example.com`).
- If it is more important to get the `sourceHostname` parameter value (`kuma.example.com`), then `sourceHostname` → `sourceAssetID` must be specified first followed by `sourceAddress` → `sourceAssetID`.
- If you specify `sourceAddress` + `sourceHostname` → `sourceAssetID`, there will be no enrichment.

Possible parameter values in the field mapping table

KUMA field	KUMA event field to write to

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

Running this script allows to do the following:

- When working with events, you can open the properties of an asset and view detailed information, such as asset vulnerabilities and the status of its antivirus protection.
- In search requests, widgets, and reports, you can use the enrich_assets and lookup_assets functions.
- You can use `inCategory` conditions in correlation rule selectors, which allow correlation logic to consider arbitrary asset properties, for example, to track internet traffic for a category of IoT devices such as webcams, coffee machines, or refrigerators.
- Alerts are assigned a severity based on the severity of the asset categories. For example, if an alert contains an asset in the Vulnerable category, the alert is assigned high severity.
- You will be able to create and export to a CSV file a list of assets that match a search filter, for example, a list of coffee machines with unpatched vulnerabilities.

Enriching events with geodata

Some events received by Kaspersky SIEM contain public IP addresses. You may need information about which geolocations correspond to the public IP addresses in the events.

To solve this problem, you can use event enrichment with geodata.

To configure event enrichment with geodata:

1. Convert geodata to the KUMA format.
2. Import the converted geodata into Kaspersky SIEM.
3. Create an enrichment rule of **the geodata** type in one of the following ways:
   - At the **Enrichment** step of the Collector Installation Wizard.
   - Similarly to the previous method, in the **Event enrichment** section in the properties of an already installed collector.
   - Separately as a resource.
4. If you have created a geodata enrichment rule separately as a resource, add it in the properties of collectors that process events with public IP addresses.
5. Update the configurations of the collectors to which you have added a geodata enrichment rule.

Geodata format

Geodata can be uploaded to Kaspersky SIEM as a CSV file in UTF-8 encoding (see the table below). A comma is used as the delimiter. The first row of the file contains the field headers: `Network`, `Country`, `Region`, `City`, `Latitude`, `Longitude`.

CSV file description

Field header name in CSV	Field description	Example
`Network`	IP address in one of the following formats: • Single IP address • Range of IP addresses • IP address in CIDR format. IPv4 and IPv6 addresses can be mixed. Required field.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Country designation used by your organization. For example, this could be its name or code. This field is required.	• `Russia` • `RU`
`Region`	Region designation used by your organization. For example, this could be its name or code.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	City designation used by your organization. For example, this could be its name or code.	• `Yekaterinburg` • `65701000001`
`Latitude`	Latitude of the described location in decimal format. This field can be empty. In this case the "0" value will be used when importing data into KUMA.	`56.835556`
`Longitude`	Longitude of the described location in decimal format. This field can be empty. In this case the "0" value will be used when importing data into KUMA.	`60.612778`

Converting geographic data from MaxMind to IP2Location

If the source files contain a different set of fields than the one indicated in this section, or if some fields are missing, the missing fields in the target CSV file will be empty after conversion.

KUMA can use geodata from MaxMind, IP2Location, or others in a format compatible with these. Prior to use, the archives with CSV geodata files need to be converted to the format supported by the solution. The names of CSV files being converted inside archives must match the following templates:

- `(GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Blocks-IPv(4|6).csv`
- `(GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Locations-%s.csv`

CSV files with geodata must not contain duplicate records. For example, if a file has few columns, different records may contain data from the same network with the same geodata. Such files cannot be converted. To successfully perform the conversion, make sure that there are no duplicate rows and that every row has at least one unique field.

Conversion can be done using a script downloaded via the link:

Download script

> Python 2.7 or later is required to run the script.

Script start command

```
python converter.py --type <geographic_data_type> --out <directory> --input <path>
```

where:

`<geographic_data_type>` is the type of geodata being processed: ("maxmind" or "ip2location")

`<directory>` is the directory in which the CSV file with geodata in KUMA format will be placed

`<path>` is the path to the ZIP archive with geodata from MaxMind or IP2location

When the script is run with the `--help` flag, a help is displayed for the available script parameters:

```
python converter.py --help
```

The command for converting a file containing a Russian database of IP address ranges from a MaxMind ZIP archive:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out geoip_maxmind_ru.csv
```

If the `--lang` parameter is not specified, the script receives information from the `GeoLite2-City-Locations-en.csv` file from the ZIP archive by default. Absence of the `--lang` parameter for MaxMind is equivalent to the following command:

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

The command for converting a file from an IP2Location ZIP archive

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
```

The command for converting a file from several IP2Location ZIP archives

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --
out geoip_ip2location_ipv4_ipv6.csv
```

The `--lang` parameter is not used for IP2Location.

Required sets of fields

The original MaxMind GeoLite2-City-Blocks-IPv4.csv and GeoLite2-City-Blocks-IPv6.csv files must contain the following set of fields: network, geoname_id, registered_country_geoname_id, represented_country_geoname_id, is_anonymous_proxy, is_satellite_provider, postal_code, latitude, longitude, accuracy_radius

```
Example set of source data:

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius
1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000
1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

The rest of CSV files with a localization code must contain the following set of fields: `geoname_id`, `locale_code`, `continent_code`, `continent_name`, `country_iso_code`, `country_name`, `subdivision_1_iso_code`, `subdivision_1_name`, `subdivision_2_iso_code`, `subdivision_2_name`, `city_name`, `metro_code`, `time_zone`, `is_in_european_union`

```
Example set of source data:

geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,subdivision_1_iso_code,subdivision
1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0
7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

The source IP2Location files must contain the network range details: `Country`, `Region`, `City`, `Latitude`, `Longitude`.

```
Example set of source data:

"0","16777215","-","-","-","-","0.000000","0.000000","-","-"
"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"
"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+08:00"
```

Importing and exporting geographic data

You can manually import and export geodata. Geodata is imported from and exported to a CSV file. If the geographic data import is successful, the previously added data is overwritten and an audit event is generated in Kaspersky SIEM.

To import geodata:

1. Prepare a CSV file containing geographic data.

   Geographic data received from MaxMind and IP2Location must be converted to a supported format.

2. In the web interface, open the **Settings** → **Other** → **General** section.

3. Under **Geographic data**, click the **Import from file** button and select a CSV file containing geographic data.

   Wait for the geographic data import to finish. The data import is interrupted if the page is refreshed.

Geodata will be uploaded to Kaspersky SIEM.

To export geodata:

1. In the web interface, open the **Settings** → **Other** → **General** section.

2. Under **Geographic data**, click the **Export** button.

   Geographic data will be downloaded as a CSV file named `geoip.csv` (in UTF-8 encoding) based on the settings of your browser.

The data is exported in the same format as it was uploaded, with the exception of IP address ranges. If a range of addresses was specified in the `1.0.0.0/24` format in the file imported into Kaspersky SIEM, then the range has the `1.0.0.0` - `1.0.0.255` format in the exported file.

Default mapping of geographic data

If you select the `SourceAddress`, `DestinationAddress` and `DeviceAddress` event fields as an IP address source when configuring a geographic data enrichment rule, the **Apply default mapping** button becomes available. You can use this button to add pre-configured mapping pairs of geographic data attributes and event fields (see the tables below).

Default mappings for the SourceAddress event field

Geodata attribute	Event field
Country	`SourceCountry`
Region	`SourceRegion`
City	`SourceCity`
Latitude	`SourceLatitude`
Longitude	`SourceLongitude`

Default mappings for the DestinationAddress event field

Geodata attribute	Event field
Country	`DestinationCountry`
Region	`DestinationRegion`
City	`DestinationCity`
Latitude	`DestinationLatitude`
Longitude	`DestinationLongitude`

Default mappings for the DeviceAddress event field

Geodata attribute	Event field
Country	`DeviceCountry`
Region	`DeviceRegion`
City	`DeviceCity`
Latitude	`DeviceLatitude`
Longitude	`DeviceLongitude`

Enriching events with data from Active Directory

Some events received by Kaspersky SIEM contain user data. If your organization uses Active Directory and users may have service accounts in addition to their primary accounts, you may need information about all accounts for each user.

To solve this problem, you can use event enrichment with data from Active Directory.

To configure event enrichment with data from Active Directory:

1. Configure a connection to the Active Directory catalog service over the LDAP protocol for the required tenant.

2. Import Active Directory data into Kaspersky SIEM.

3. At the **Event enrichment** step of the Collector Installation Wizard, or in the properties of an existing collector for the tenant for which the connection was configured in step 1, configure LDAP enrichment.

4. Update the configuration of the collector for which you configured enrichment using LDAP.

To learn more about the event enrichment using LDAP, watch this video:

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

When you configure event enrichment with data from Active Directory, you can do the following:

- When working with events, you can open user account cards.

- In search requests, widgets, and reports, you can use the enrich_accounts and lookup_accounts SQL functions.

- You can use domain group `DistinguishedName` correlation rules in selectors, for example, the condition `SourceAccountID inActiveDirectoryGroup CN=admins,OU=Users,DC=example,DC=com`.

Enriching events with DNS names

Some events received by KUMA contain IP addresses. For easier event analysis, you may need information about which DNS names correspond to IP addresses in events.

To solve this problem, you can use event enrichment with DNS names.

To configure event enrichment with DNS names:

1. Create an enrichment rule of the **DNS** type in one of the following ways:

   - at the **Event enrichment** step of the Collector Installation Wizard;

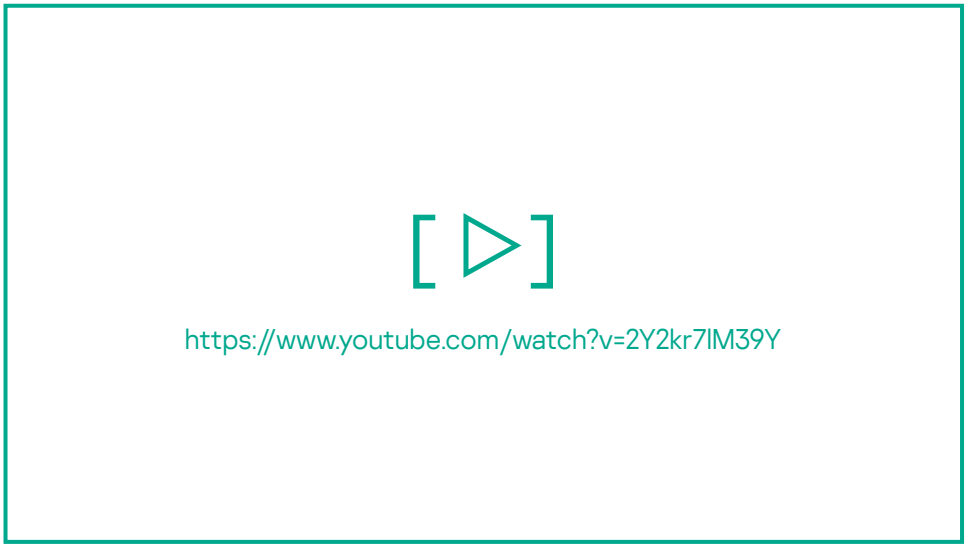
   - in the properties of an already installed collector in the **Event enrichment** section;

   - separately as a resource.

2. If you have created a DNS name enrichment rule separately as a resource, add it in the properties of the collectors that process events with public IP addresses.

3. Update the configurations of the collectors to which you have added the DNS name enrichment rule.

To learn more about the enrichment of events with data from DNS server, watch this video:



Enriching events using a dictionary

Some event sources, transmit event field values as codes. However, analyzing events may require mapping descriptions to codes. For example, code 1001 may correspond to "Failed authorization".

To turn codes into text values in KUMA, you can use event enrichment with a dictionary. The dictionary maps a value to each code. In the normalizer, an enrichment rule is configured with the **dictionary** data source type.

When processing an event, the value of a field is used as the key to look up the corresponding entry in the dictionary. The value obtained from the dictionary is written to the specified target field of the normalized event. For example, if the `event_code` field in the original event contains the value 1001, and in the dictionary this code is mapped to "Failed authorization", after the event is processed, the `Name` field contains "Failed authorization".

Before you begin, make sure the following conditions are satisfied:

- The event source passes the code in a certain field, such as `event_code`.
- KUMA has a normalizer for events of this source.
- A list of codes and matching descriptions has been prepared.

Configuring event enrichment using a dictionary involves the following steps:

1 Creating a dictionary

A dictionary contains key-value pairs. The event code is used as the key, and the description is used as the value.

To create a dictionary:

1. In the KUMA web interface, go to the **Resources** → **Dictionaries** section.
2. Create a dictionary of the **Dictionary** type.
3. Add entries to the dictionary that contain an event code and a description.
4. Save the dictionary.

The dictionary may contain entries such as the following:

Examples of dictionary entries

Key	Value
1001	Failed authorization
1002	Successful authorization
1003	Changing a password

The dictionary must contain all codes that you want to use in event enrichment.

2 Configuring enrichment in the normalizer

After creating a dictionary, you need to configure an enrichment rule in the normalizer.

To configure an enrichment rule:

1. In the KUMA web interface, select **Resources** → **Normalizers**.
2. Open the settings for the normalizer that processes events from the source.
3. Go the **Enrichment** tab.
4. Click the **Add enrichment** button.
5. In the **Source kind** drop-down list, select **dictionary**.
6. In the **Dictionary name** field, select the previously created dictionary.
7. In the **Target field** drop-down list, select **Name**.
8. In the **Key fields** drop-down list, select the source event field that contains the event code, such as `event_code`.
9. If necessary, select the **Debug** check box to log the workings of the enrichment rule in greater detail in the normalizer log.
10. Click **OK**.
11. Save the changes for the normalizer.

When processing an event, the value of the `event_code` field is used as the key to look up an entry in the selected dictionary. The value of the found entry is written to the `Name` field of the normalized event. For example, if the value of the `event_code` field in the original event is `1001`, and the dictionary maps `Failed authorization` to code `1001`, after enrichment, the `Name` field of the normalized event is set to `Failed authorization`.

3 Testing event enrichment

After changing settings, you need to send a test event to KUMA containing a code that is present in the dictionary.

To test enrichment:

1. Send a test event containing a value in the `event_code` field via the collector.
2. In the KUMA web interface, go to the **Events** section.
3. Find the processed test event.
4. Check the value of the `Name` field.

If the value in the `Name` field is missing or is not what you expected, check the following:

- The dictionary does contain an entry with the corresponding key.
- The field that contains the event code is selected in the **Key fields** drop-down list.
- The `Name` field is specified as the target field.
- The modified normalizer has been saved and is being used by the collector that processes the test event.

4 Updating the dictionary (optional)

When you add new codes or change descriptions, update the corresponding entries in the dictionary.

To update the contents of a dictionary:

1. In the KUMA web interface, go to the **Resources** → **Dictionaries** section.
2. Open the dictionary used for enrichment.
3. Add new or edit existing entries.
4. Save your changes.

The enrichment configured in the normalizer continues to use this dictionary. You do not need to recreate enrichment rules after editing dictionary entries. KUMA converts the codes specified in the original events into their corresponding text values and writes these to the `Name` field of the normalized event.

Event routing

An event router is a service that allows you to receive streams of events from collectors and correlators and then distribute the events to specified destinations in accordance with the configured filters.

To have events from the collector sent to the event router, you must create an 'eventRouter' destination resource with the address of the event router and link the resource to the collectors that you want to send events to the event router.

The event router receives events on the API port, just like 'storage' and 'correlator' destinations.

You can create a router in the **Resources** section.

Using an event router allows you to reduce the utilization of links, which is important for low-bandwidth and traffic-busy links.

The event router must be installed on a Linux device. Only a user with the General Administrator role can create the service. You can create a service in any tenant; the tenant relation does not impose any restrictions.

You can install the event router service on a separate host or together with a collector or correlator. There is no separate section for the event router in the inventory file, so you can specify the host on which you want to install the event router in the `kuma_collector` or `kuma_correlator` section. Also, if you want to install the event router on a separate host, you need to specify this host in the inventory file in the `kuma_collector` or `kuma_correlator` section; in this way, the event router service will be upgraded as part of the next KUMA upgrade.

You can use the following metrics to get information about the service performance:

- IO
- Process
- OS

As with other resources, the following audit events are generated for the event router in KUMA:

- Resource was successfully added
- Resource was successfully updated
- Resource was successfully deleted

Installing an event router involves two steps:

- Create the event router service in the KUMA web interface using the Installation Wizard.
- Install the event router service on the server.

Starting the Event Router Installation Wizard

To start Event Router Installation Wizard:

1. In the KUMA web interface, in the **Resources** section, click **Event routers**.

2. This opens the **Event routers** window; in that window, click **Add**.

Follow the instructions of the installation wizard.

Step 1. General settings of the event router

This is a required step of the Installation Wizard. At this step, you specify the main settings of the event router: its name and the tenant that will own it.

To specify the general settings of the event router:

1. On the **Basic settings** tab, fill in the following fields:

   a. In the **Name** field, enter a unique name for the service you are creating. The name must contain 1 to 128 Unicode characters.

   b. In the **Tenant** drop-down list, select the tenant that will own the event router. An event router belonging to a tenant is organizational in nature and does not impose any restrictions.

   c. If necessary, specify the number of processes that the service can run concurrently in the **Handlers** field. By default, the number of handlers is the same as the number of vCPUs on the server where the service is installed.

   d. You can optionally add up to 4000 Unicode characters describing the service in the **Description** field.

2. On the **Advanced settings** tab, fill in the following fields:

   a. If necessary, use the **Debug** toggle switch to enable logging of service operations.

   b. You can use the **Create dump periodically** toggle switch at the request of Technical Support to generate resource (CPU, RAM, etc.) utilization reports in the form of dumps.

   c. In the **Dump settings** field, you can specify the settings to be used when creating dumps. For instructions on filling out this field, please contact Technical Support.

General settings of the event router are specified. Proceed to the next step of the Installation Wizard.

Step 2. Routing

This is a required step of the Installation Wizard. We recommend sending events to at least two destinations: to the correlator for analysis and to the storage for storage. You can also select another event router as the destination.

To specify the settings of the destination to which you want the event router to send events received from collectors:

1. In the **Routing** step of the Installation Wizard, click **Add**.

2. This opens the **Create destination** window; in that window, specify the following settings:

   a. On the **Basic settings** tab, in the **Name** field, enter a unique name for the destination. The name must contain 1 to 128 Unicode characters.

   b. You can use the **State** toggle switch to enable or disable the service as needed.

   c. In the **Type** drop-down list, select the type of the destination. The following values are available:

      - nats-jetstream
      - tcp
      - http
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. On the **Advanced settings** tab, specify the values of parameters. The set of parameters that can be configured depends on the type of the destination selected on the **Basic settings** tab. For detailed information about parameters and their values, click the link for each type of destination in paragraph "c." of these instructions.

The created destination is displayed on the Installation Wizard tab. A destination resource can be removed from the resource set by selecting it and clicking **Delete** in the opened window.

Routing is configured. You can proceed to the next step of the Installation Wizard.

Step 3. Setup validation

This is the required, final step of the Installation Wizard.

To create an event router in the Installation Wizard:

1. Click **Create and save service**.

   The lower part of the window displays the command that you must use to install the router on the server.

   Example command:

   ```
   /opt/kaspersky/kuma/kuma eventrouter --core https://kuma-example:<port used for
   communication with the KUMA Core> --pair.fingerprint <fingerprint ID of the KUMA Core CA
   certificate> --id <service ID> --api.port <port used for communication with the event
   router service> --install
   ```

where:

`< fingerprint ID of the KUMA Core CA certificate >` is the fingerprint ID of the CA certificate used for authentication when connecting the service.

The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

The port for communication with the KUMA Core, the service ID, the fingerprint ID of the KUMA Core CA certificate, and the port for communication with the service are added to the command automatically. You must also ensure the network connectivity of KUMA and open the ports used by solution components, if necessary.

2. Close the Wizard by clicking **Save**.

The service is installed in the KUMA web interface. You can now proceed with installing the service in the KUMA network infrastructure.

Installing the event router on the server

To install the event router on the server:

1. Log in to the server where you want to install the event router service.

   If you want to install the event router service on a separate server, specify the host in the inventory file in the `kuma_correlator` group and install the router service on that host. When upgrading KUMA, the installer upgrades the event router installed on the host specified in the inventory file.

2. Create the /opt/kaspersky/kuma/ directory.

3. Copy the `kuma` file to the /opt/kaspersky/kuma directory. The file is located inside the installer in the /kuma-ansible-installer/roles/kuma/files directory.

4. Make sure the `kuma` file has the execute permission. If the file is not executable, make it executable:

```
sudo chmod +x /opt/kaspersky/kuma/kuma
```

5. Place the `LICENSE` file from the /kuma-ansible-installer/roles/kuma/files/ directory in the /opt/kaspersky/kuma/ directory and accept the terms and conditions of the End User License Agreement by running the following command:

```
sudo /opt/kaspersky/kuma/kuma license
```

6. Create the 'kuma' user:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

7. Make the 'kuma' user the owner of the /opt/kaspersky/kuma directory and all files inside the directory:

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

8. Add the KUMA event router port to firewall exclusions.

> For the solution to work correctly, ensure that the KUMA components are able to interact with other components and applications over the network via the protocols and ports specified during the installation of the KUMA components.

9. Execute the following command:

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --api.port <API_port> --install
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the router ID copied from the KUMA web interface.
- <API_port> is the port used for communication with the component being installed.

Example:

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id
XXXX --api.port YYYY --install
```

The event router is installed on the server. You can use it to receive events from collectors and relay the events to specified destinations.

Use case: the collector sends events to a router in a data center

The collector sends events to an event router in the data center, and the event router sends the events to the specified destinations: a correlator and storage.

A company has multiple branch offices. All KUMA components are deployed in the data center. Multiple collectors are deployed in the branch offices. Each collector must send data from the branch office to the storage and the correlator in the data center. Some branch offices do not have a broadband connection to the data center.

In this case, you can install an event router in the data center and direct the data from each branch collector to the event router rather than directly to the storage and the correlator. Having one data stream instead of two reduces the load on the weak data link.

The events are delivered to the storage and the correlator on the data center side. To achieve this, you need to specify the storage and correlator destinations in the properties of the event router.

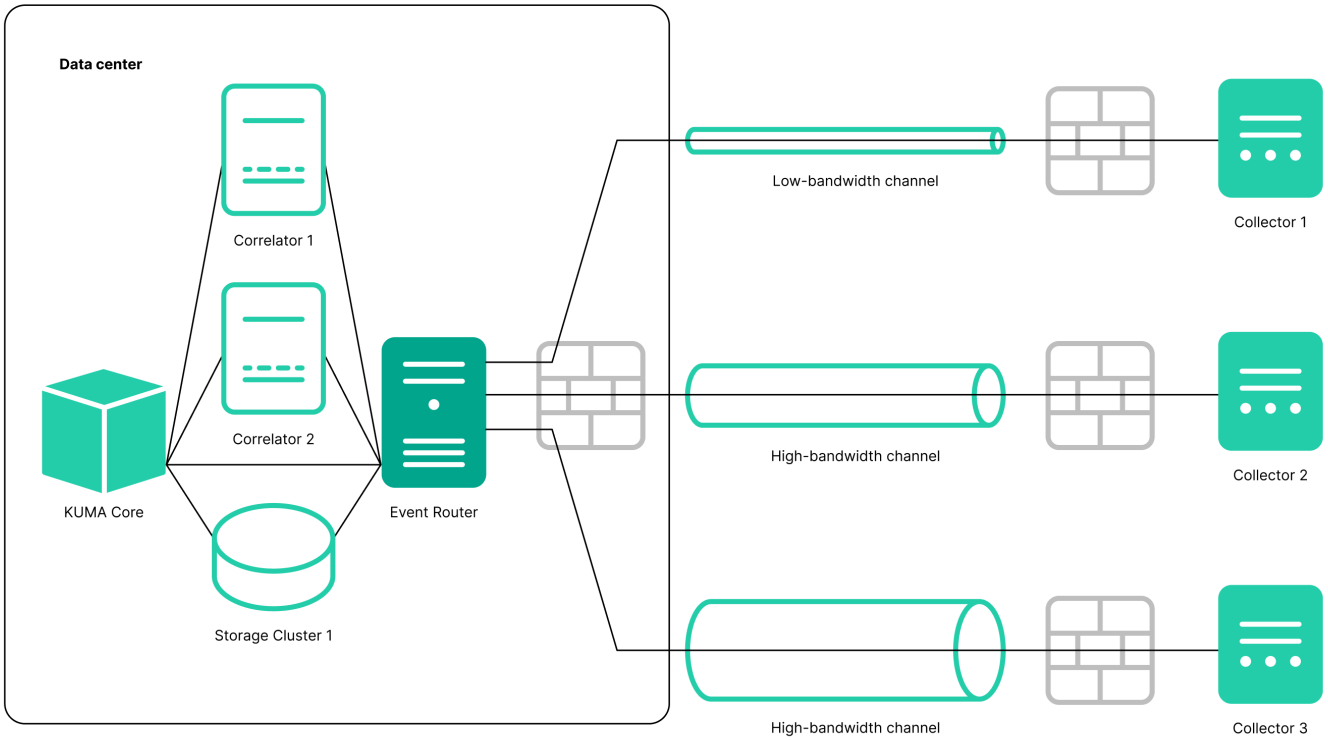


Diagram of router connection in the data center

Prerequisites

- Collectors are configured in the branches.
- The data center has sufficient capacity to install an event router.
- KUMA is installed in the data center.

Steps

Configuring the event router involves the following steps:

1. **Creating the storage and correlator destinations**

   If you have not yet created destinations of the **storage** and **correlator** types in the data center, create these. Specify the storage URL and the correlator URL in the settings of the destinations.

2. **Installing and configuring the event router service in the data center infrastructure**

   To install the event router service:

   1. Create an event router service in the KUMA web interface. In the **Routing** section, add destinations of the **storage** and **correlator** types for the storage and correlator in your data center.

   2. Install the event router service on the server.

3. **Creating a destination for the event router**

   Create a destination of the **eventRouter** type. In the destination settings, specify the URL of the event router in your data center.

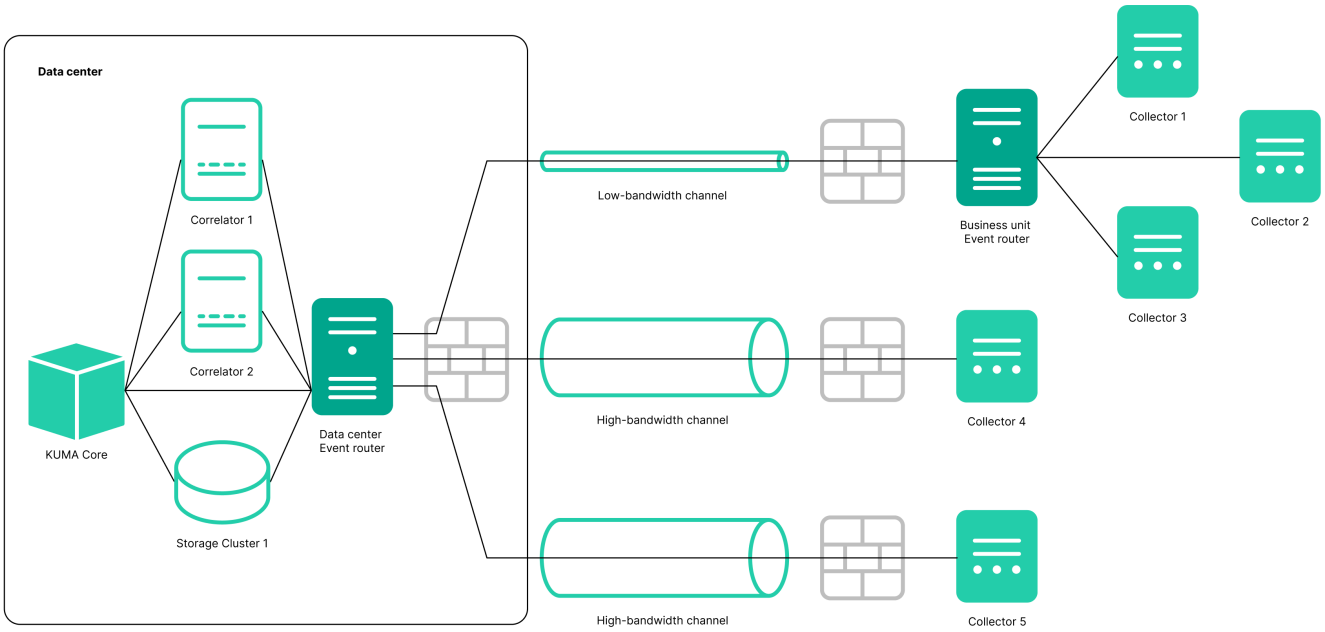
4. **Configuring collectors in branch offices to send events to the event router in the data center**

   In collector properties, in the **Routing** section, specify the event router destination that you just created.

Data from branch offices is sent to the data center as one stream, which reduces the load on weak data links.

Use case: cascade of event routers

Multiple collectors send events to an event router in a branch office. The event router in the branch office forwards events to the router in the data center, and from there, the events are routed to the configured destinations, that is, correlators and storage.



Router cascade diagram

Prerequisites

- Collectors are configured in the branches.
- The data center has the capacity to install an event router.
- KUMA is installed in the data center.

Stages

Configuring an event router cascade involves the following steps:

1. **Configuration at the data center:**

At the data center:

1. Create an event router service.
2. Create destination points of the **storage** and **correlator** types and specify these in the event router.
3. In the event router, on the **Advanced settings** tab, configure a filter to send events to a storage and/or correlator, for example, `DeviceCustomString` = `correlator` or `DeviceCustomString` = `storage`.

2. **Configuration at the branch office**

   At the branch office:

   1. Create an event router service.
   2. Create a destination of the **eventRouter** type and specify the URL of the event router at the data center.
   3. Create a destination of the **eventRouter** type and specify the URL of the event router at the branch office.

      If **eventRouter** replaces previously configured destinations, you may delete them.

Event routers are configured at the data center and the branch offices. Collectors are also configured at the branch office.

The connection of branch offices to the data center is optimized. Now it is no longer required to configure sending of the events to the data center in each collector. It is sufficient to collect a unified event stream at the router, and send it to the data center as a single stream.

Creating and using KUMA agents

KUMA *agents* are services that forward raw events from servers and workstations to KUMA destinations.

The following types of agents are provided:

- wmi agents are used to receive data from remote Windows devices using Windows Management Instrumentation. These are installed on Windows devices.
- wec agents are used to receive Windows logs from a local device using Windows Event Collector. They are installed to Windows assets.
- tcp agents receive data over TCP. These are installed on Linux and Windows devices.
- udp agents receive data over UDP. They are installed to Linux and Windows assets.
- nats-jetstream—used for NATS communications. They are installed to Linux and Windows assets.
- kafka agents are used for kafka communications. They are installed to Linux and Windows assets.
- http agents are used for communication over HTTP. They are installed to Linux and Windows assets.
- file agents get data from a file. They are installed to Linux and Windows assets.
- ftp agents receive data over the File Transfer Protocol. They are installed to Linux and Windows assets.
- nfs agents receive data over the Network File System protocol. They are installed to Linux and Windows assets.

- snmp agents receive data using the Simple Network Management Protocol. They are installed to Linux and Windows assets.
- diode agents are used together with data diodes to receive events from isolated network segments. They are installed to Linux and Windows assets.
- etw agents receive Event Tracing for Windows data. They are installed to Windows assets.

Creating an agent involves the following stages:

1. Creating a resource set for the agent in the web interface
2. Creating an agent service in the web interface
3. Installing the server portion of the agent to the asset that will send events

KUMA agents for Windows devices can be created as follows:

- Manually by creating a set of agent resources and creating an agent service in the KUMA web interface.
- Create automatically when creating a collector of the wmi, wec, or etw transport type. Although the set of resources and service of these agents are created in the Collector Installation Wizard, they must still be installed to the asset that will be used to send an event. In a manually created agent, a connector of the etw type can be used in only one connection. If you configure multiple connections in a manually created etw agent, the status of the etw agent status is green, but events are not transmitted and an error is logged in the etw agent log.

Multiple agents can be installed on a device; the version of all such agents must be the same.

If an older version of the agent is already installed on the device where you want to create an agent, you must first stop the installed agent (remove the agent from a Windows device or restart the agent service on a Linux device), and then you can proceed to create a new agent. However, if the version of the installed agents is the same as the version of the agent that you want to create, stopping the agents is not necessary.

When creating and running an agent whose version is 3.0.1 or later, you must accept the terms and conditions of the End User License Agreement.

In a configuration with KUMA Core services in a Raft cluster, all agent management operations (for example, restarting) must be performed from the host to which the agent is currently connected. The agent connects to the first available KUMA Core from the list of hosts specified in the agent's configuration. Therefore, before performing the operation, you need to determine which KUMA Core the agent is connected to and perform the operation from the corresponding host. For example, if hosts are listed in the agent configuration in the order of 3, 2, 1, and host 3 is unavailable, the agent connects to the KUMA Core on host 2. In this case, all agent management operations must be performed from host 2.

Creating a set of resources for an agent

In the KUMA web interface, an agent service is created based on the resource set for an agent that combines connectors and destinations. The agent type is determined by the connector that is used in the agent. The only exception is for agents with a destination of the diode type. These agents are considered to be diode agents.

To create a resource set for an agent in the KUMA web interface:

1. In the KUMA web interface, under **Resources** → **Agents**, click **Create new**.

   This opens the agent creation window. The left part of the window displays tabs with base settings of the agent and connections. The **Base settings** tab is active.

2. On the **Base settings** tab:

   - In the **Name** field, enter a unique name for the service you are creating. The name must contain 1 to 128 Unicode characters.
   - In the **Tenant** drop-down list, select the tenant that will own the storage.
   - If you want to enable logging of service operations, enable the **Debug** toggle switch.
   - If you want to view the names of services or addresses of hosts from which the event came, enable the **Track event route** toggle switch.

     The **Track event route** toggle switch is available if at least one **internal** destination is specified in the connections. By default, the toggle switch is **Disabled**.
   - You can optionally add up to 256 Unicode characters describing the service in the **Description** field.

3. Go to the tab of an existing connection or create a connection by clicking the **Add** button in the lower part of the left pane, then go to the tab of the newly created connection to edit its settings.

   By default, a connection named **Config #1** is created for a new agent. The name of the connection follows the **Config #<number>** pattern.

   You can create multiple connections for an agent. If necessary, you can manage connections:

   - Rename connections
   - Duplicate connections
   - Delete connections

4. If necessary, in the **Name of connection** field, rename the connection for your convenience when managing it, for example, to be able to figure out from which connection and from which agent events arrived. If you leave the field blank, a name is assigned following the **Config #<number>** pattern.

   The name can contain from 1 to 128 characters. The name can contain only letters and numerals and cannot contain special characters. Leading and trailing spaces are removed. When pasting a name into the field from the clipboard, if the text contains a newline, paragraph, or indentation, these characters are replaced with a space. You can reuse a name for multiple connections within the same agent.

   If you have enabled event route tracing, then when viewing event information, the **Events** section displays the name of the connection from which the event was received.

5. In the **Connector** group of settings, add a connector:

- If you want to select an existing connector, select it from the drop-down list.
- If you want to create a new connector, select **Create new** in the drop-down list and specify the following settings:
  - Specify the connector name in the **Name** field. The name must contain 1 to 128 Unicode characters.
  - In the **Type** drop-down list, select the connector type and specify its settings on the **Basic settings** and **Advanced settings** tabs. The available settings depend on the selected type of connector:
    - tcp
    - udp
    - nats-jetstream
    - kafka
    - http
    - file
    - ftp
    - nfs
    - wmi
    - wec
    - snmp
    - snmp-trap
    - etw
    - kata/edr
    - office365
    - dfi
    - vmware
    - 1c-log
    - 1c-xml

    When using the **tcp**, **udp**, **http**, **wec**, **wmi**, **etw** connector type at the normalization stage, IP addresses of the assets from which the events were received will be written in the DeviceAddress event field if it is empty.

> The ability to edit previously created wec, wmi, or etw connections in agents, collectors, and connectors is limited. You can change the connection type from **wec** to **wmi** or **etw** and back, but you cannot change the **wec**, **wmi**, or **etw** connection to any other connection type. When editing other connection types, you cannot select the **wec**, **wmi**, or **etw** types. You can create connections without any restrictions on the types of connectors.

> When adding an (existing or new) wmi, wec, or etw connector for an agent, the **TLS mode** and **Compression** settings are not displayed on the agent, but the values of these settings are stored in the agent's configuration. For a new connector, these settings are disabled by default.
> If TLS mode is enabled for an existing connector that is selected in the list, you cannot download the agent configuration file. In this case, to download the configuration file, you must go to the connector resource that is being used on the agent and disable TLS mode.

The connector is added to the selected connection of the agent's resource set. The created connector is only available in this resource set and is not displayed in the web interface **Resources** → **Connectors section**.

6. In the **Destinations** group of settings, add a destination.

   - If you want to select an existing destination, select it from the drop-down list.
   - If you want to create a new destination, select **Create new** in the drop-down list and specify the following settings:
     - Specify the destination name in the **Name** field. The name must contain 1 to 128 Unicode characters.
     - In the **Type** drop-down list, select the destination type and specify its settings on the **Basic settings** and **Advanced settings** tabs. The available settings depend on the selected type of destination:
       - **nats-jetstream**—used for NATS communications.
       - **tcp**—used for communications over TCP.
       - **http**—used for HTTP communications.
       - **diode**—used to transmit events using a data diode.
       - **kafka**—used for Kafka communications.
       - **file**—used for writing to a file.
     - Enable or disable the **State** toggle switch to enable or disable the sending of events to the destination. This toggle switch is turned on by default.

   > The advanced settings for an agent destination (such as TLS mode and compression) must match the advanced destination settings for the collector that you want to link to the agent.

   There can be more than one destination point. You can add them by clicking the **Add destination** button and can remove them by clicking the ✕ button.

7. Repeat steps 3–5 for each agent connection that you want to create.

8. Click **Save**.

The resource set for the agent is created and displayed under **Resources** → **Agents**. Now you can create an agent service in KUMA.

Managing connections for an agent

You can manage the connections created for the agent by renaming, duplicating, or deleting them.

Renaming a connection

By default, the name of a new connection created in a resource set for an agent follows the **Connection <number>** pattern. For your convenience when managing connections, you can rename them, for example, to make it clear at a glance from which connection and from which agent an event was received.

To rename a connection:

1. In the KUMA web interface, in the **Resources** → **Agents** section, create a new agent or click an existing agent in the table.
2. If necessary, create a connection for the agent by clicking the **Add** button in the lower part of the left pane.
3. Go to the tab of the connection that you want to rename.
4. In the **Connection name** field, edit the name of the connection.

   The name can contain from 1 to 128 characters. The name can contain only letters and numerals and cannot contain special characters. Leading and trailing spaces are removed. When pasting a name into the field from the clipboard, if the text contains a newline, paragraph, or indentation, these characters are replaced with a space. You can reuse a name for multiple connections within the same agent.
5. Click **Save**.

The connection is renamed. If you have enabled event route tracing, then when viewing event information, the **Events** section displays the name of the connection from which the event was received.

Duplicating a connection

If you want to create a connection for an agent based on an existing connection, you can create a copy of the connection with identical settings.

To duplicate a connection:

1. In the KUMA web interface, in the **Resources** → **Agents** section, create a new agent or click an existing agent in the table.

2. If necessary, create a connection for the agent by clicking the **Add** button in the lower part of the left pane.

3. Go to the tab of the connection that you want to duplicate and click the **Duplicate** button.

   A connection is created for the agent with the same settings as the original connection. The new connection is created with one of the following names:

- If the original connection name followed the **Connection <number>** template, the duplicated connection name also follows this template. The connection is named "Connection <number+1>", where <number> is the number of the last created connection whose name followed the same template.

- If the original connection had been renamed, the new connection gets the same name. You can reuse a name for multiple connections within the same agent.

You can edit the name of the new connection in the **Name of connection** field on the tab of the connection.

Removing a connection

If the agent has more than one connection, you can delete a connection.

To delete a connection:

1. In the KUMA web interface, in the **Resources** → **Agents** section, create a new agent or click an existing agent in the table.

2. If necessary, create a connection for the agent by clicking the **Add** button in the lower part of the left pane.

3. Go to the tab of the connection that you want to delete and click the **Delete** button.

   You cannot restore a deleted connection, but you can recover the version of the agent in which this connection was previously saved through the change history.

Creating an agent service in the KUMA web interface

When a resource set is created for an agent, you can proceed to create an agent service in KUMA.

To create an agent service in the KUMA web interface:

1. In the KUMA web interface, under **Resources** → **Active services**, click **Add service**.

2. In the opened **Choose a service** window, select the resource set that was just created for the agent and click **Create service**.

The agent service is created in the KUMA web interface and is displayed under **Resources** → **Active services**. Now agent services must be installed to each asset from which you want to forward data to the collector. A service ID is used during installation.

Automatically created agents

When creating a collector with wec, wmi, or etw connectors, agents are automatically created for receiving Windows events.

Automatically created agents have the following special conditions:

- Automatically created agents can have only one connection.

- Automatically created agents are displayed under **Resources** → **Agents**, and `auto created` is indicated at the end of their name. Agents can be reviewed or deleted.

- The settings of automatically created agents are defined automatically based on the collector settings from the **Connect event sources** and **Transport** sections. You can change the settings only for a collector that has a created agent.

- The description of an automatically created agent is taken from the collector description in the **Connect event sources** section.

- Debugging of an automatically created agent is enabled and disabled in the **Connect event sources** section of the collector.

- When deleting a collector with an automatically created agent, you will be prompted to choose whether to delete the collector together with the agent or to just delete the collector. When deleting only the collector, the agent will become available for editing.

- When deleting automatically created agents, the type of collector changes to **http**, and the connection address is deleted from the **URL** field of the collector.

- If at least one Windows log name in wec or wmi connector is specified incorrectly, the agent will not receive events from any Windows log listed in the connector. At the same time the agent status will be green. Attempts to receive events will be repeated every 60 seconds, and error messages will be added to the service log.

- If in a connector of the etw type, the session name is specified incorrectly, the wrong provider is specified in the session, or an incorrect method is specified for sending events (to send events correctly, on the Windows Server side, you must specify "Real time" or "File and Real time" mode), events will not arrive from the agent, an error will be recorded in the agent log on Windows, and the status of the agent will be green. At the same time, no attempt will be made to get events every 60 seconds. If you modify session settings on the Windows side, you must restart the etw agent and/or the session for the changes to take effect.

In the KUMA interface, automatically created agents appear at the same time when the collector is created. However, they must still be installed on the asset that will be used to send a message.

Installing an agent in a KUMA network infrastructure

When an agent service is created in KUMA, you can proceed to installation of the agent to the network infrastructure assets that will be used to forward data to a collector.

Multiple agents can be installed on a device; the version of all such agents must be the same.

> Prior to installation, verify the network connectivity of the system and open the ports used by its components.

Installing a KUMA agent on Linux assets

KUMA agent installed on Linux devices stops when you close the terminal or restart the server. If you do not want to start KUMA agents manually, we recommend installing agents using an application that automatically starts applications whenever the server is restarted, for example, the Supervisor application. If you want to start KUMA agents automatically, specify the automatic start and restart settings in the KUMA configuration file. For more information on configuring automatic starting and restarting, see the official documentation of applications for automatically starting applications.

Example configuration in Supervisor

```
[program:agent_<agent_name>] command=sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port>
autostart=true
autorestart=true
```

where:

- <agent_name> is the name of the KUMA agent.
- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port number of the KUMA Core.

To install a KUMA agent to a Linux asset:

1. On the Linux device on which you want to install the KUMA agent, create directories for the KUMA configuration file and agents, for example:
   - /opt/kaspersky/kuma
   - /opt/kaspersky/agent
2. Place the KUMA configuration file in the directory created for it. The KUMA configuration file can be found inside the installer in the /kuma-ansible-installer/roles/kuma/files directory.

   > Make sure the kuma file has sufficient rights to run.

3. Create the KUMA user:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

4. Grant the KUMA user access to the directory with the KUMA configuration file and to all files within the directory:

```
sudo chown -R kuma:kuma <path>
```

where:

<path> is the path to the directory with the KUMA configuration file.

5. Install the KUMA agent:

```
sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --wd <path> [--accept-eula]
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service. The `--pair.fingerprint` argument is optional.

  You can install the service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  If you want to specify the fingerprint ID for validation of KUMA Core's CA certificate, go to the **Resources and services** → **Active services** section, and select the check box next to the KUMA Core service; in the menu (⋮), select **Copy certificate fingerprint**, then use the copied fingerprint ID in the agent installation command. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the service ID copied from the KUMA web interface.
- <path> is the path to the directory for the files of the KUMA agent that is being installed. If this option is not specified, the files are stored in the directory where the kuma file is located.

You can install two KUMA agents on the same Linux device. In this case, KUMA agents will work in parallel. When installing the second KUMA agent, you need to specify a separate directory for it using the `--wd` option.

To run the agent, you need to accept the End User License Agreement. You can add the `--accept-eula` option to the command to automatically accept the End User License Agreement during KUMA agent installation. This lets you perform the installation non-interactively. If you do not specify this option, you will need to accept or reject the License Agreement manually during the installation of the KUMA agent.

Examples of installing the KUMA agent:

- Installing the KUMA agent without automatically accepting the End User License Agreement:

  ```
  sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
  /opt/kaspersky/kuma/agent/XXXX
  ```

- Installing the KUMA agent with automatic acceptance of the End User License Agreement:

```
sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX --accept-eula
```

> By using the `--accept-eula` option during the installation of the KUMA agent, you confirm that you agree with and accept the terms and conditions of the End User License Agreement.

6. If you chose KUMA installation with the automatic acceptance of the End User License Agreement and want to read the text of the End User License Agreement, or if the text of the End User License Agreement was not automatically provided to you during the installation process, run the following command:

```
./agent license --show
```

The KUMA agent is installed on the Linux device.

You can configure the collector to receive data that the KUMA agent sends to KUMA.

Installing a KUMA agent on Windows assets

Before installing the KUMA agent on a Windows device, make sure that the user account under which the KUMA agent will run has the necessary rights.

Rights for a user account when installing a KUMA agent of any type

The server administrator must create a user account with the 'Log on as a service' permission on the Windows asset. This user account must be used to install the agent.

Rights for a user account when installing a KUMA agent of the wec type

The server administrator must create a user account with the 'Event Log Readers' and 'Log on as a service' permissions on the Windows asset. This user account must be used to install and start the agent.

If you plan to receive events from the Security log on a domain controller, grant access to the Security log to the preset Network Service account in Windows. To do this, run the following command on the PowerShell command line of the domain controller device:

```
wevtutil sl security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
(A;;0x1;;;S-1-5-20)'
```

> If you do not configure access to the Security log, but add the Security log in the wec connector settings, then the stream of events from the KUMA agent will not be received.

If you want to receive events from something other than a domain controller, it is sufficient to add the preset Network Service user account in Windows to the Event Log Readers group.

Rights for a user account when installing a KUMA agent of the wmi type

The server administrator must create a user account with the 'Event Log Readers' and 'Log on as a service' permissions on the Windows asset. This user account must be used to install the agent.

The 'Event Log Readers' and 'Log on as a service' permissions are required to run the agent under a domain account.

If you want to run the agent under a local account, you will need administrator rights as well as 'Event Log Readers' and 'Log on as a service' permissions.

If you want to perform remote collection of events (collection of events from devices connected to the device on which the KUMA agent is installed) and only read logs under a domain account, the 'Event Log Readers' permission is sufficient.

Rights for a user account when installing a KUMA agent of the etw type

The server administrator must create a user account with the 'Log on as a service' permission on the Windows asset. This user account must be used to install the agent.

To run the agent, the user account must have administrator rights or must be added to one of the following security groups:

- Domain admins
- Performance Log Users

Installing the KUMA agent

To install a KUMA agent to a Windows asset:

1. Copy the kuma.exe file to a folder on the Windows asset. `C:\Users\<User name>\Desktop\KUMA` folder is recommended for installation.

   The kuma.exe file is located inside the installer in the /kuma-ansible-installer/roles/kuma/files/ directory.

2. Start the Command Prompt on the Windows asset with Administrator privileges and locate the folder containing the kuma.exe file.

3. Execute the following command:

```
kuma agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID> --user <user> --
install [--accept-eula]
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service. The `--pair.fingerprint` argument is optional.

  You can install the service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If the value is `insecure`, the fingerprint does not need to be renewed after reissuing the the CA certificate.

  If you want to specify the fingerprint ID for validation of KUMA Core's CA certificate, go to the **Resources and services** → **Active services** section, and select the check box next to the KUMA Core service; in the menu (⋮), select **Copy certificate fingerprint**, then use the copied fingerprint ID in the agent installation command. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the service ID copied from the KUMA web interface.
- <user> is the user name of the user that the agent will run as, including the domain.

To run the agent, you need to accept the End User License Agreement. You can add the `--accept-eula` option to the command to automatically accept the End User License Agreement during agent installation. This lets you perform the installation non-interactively. If you do not specify this option, you will need to accept or reject the License Agreement manually during the installation of the KUMA agent.

Examples:

- Installing the KUMA agent without automatically accepting the End User License Agreement:

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install
```

- Installing the KUMA agent with automatic acceptance of the End User License Agreement:

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install --accept-eula
```

By using the `--accept-eula` option during the installation of the KUMA agent, you confirm that you agree with and accept the terms and conditions of the End User License Agreement.

You can get help information by executing the `kuma help agent` command.

4. If you started the installation of the agent without automatically accepting the End User License Agreement, during the installation process, you will be prompted to read the text of the End User License Agreement and you will have the opportunity to accept or reject the agreement.

5. If you chose installation with the automatic acceptance of the End User License Agreement and want to read the text of the End User License Agreement, or if the text of the End User License Agreement was not automatically provided to you during the installation process, run the following command:

```
kuma.exe license --show
```

If you want to accept the End User License Agreement, run the following command and press `y`:

```
kuma.exe license
```

6. Specify the password for the agent's user in one the following ways:

- Manually.

- From a file when installing the agent.

  To avoid entering the password manually, you can add the password to a .TXT file and place the file in the same directory as the executable file of the agent.

  In the command, specify the file containing the password as follows: `< name of the password file >.txt`. For example, `password.txt`.

  ```
  kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install < password.txt
  ```

  All data from the password.txt file is redirected to the command as the password, excluding end-of-line characters (\n\r, \n).

  Path for storing the agent folder after installation: C:\ProgramData\Kaspersky Lab\KUMA\agent\${agent_id}.

If you did not accept the End User License Agreement (EULA) before installing the agent with the `< password.txt` flag, an error message is displayed saying that the agreement was not accepted.

You can accept the EULA in the following ways:

a. In the password file, you can specify the EULA acceptance flag. To achieve this, the file with the password must contain two lines: the first line containing "y", which serves to assert EULA acceptance, and the second line containing the password. For example:

   `y`

   `<password>`

   The agent installation command looks like this:

   ```
   kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install < password.txt
   ```

   In this case, you will not need to additionally accept the EULA when installing the agent.

   If the EULA has been accepted before running the command with the password file, the first line in the file is interpreted as the password and the installation is aborted with an `Access denied` error.

b. You can accept the EULA and perform a silent installation at the same time by using the --accept-eula flag.

The agent installation command looks like this:

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --accept-eula --install < password.txt
```

Make sure that only the password is specified in the file, on the first line, otherwise an error will occur.

The `C:\ProgramData\Kaspersky Lab\KUMA\agent\< Agent ID >` folder is created in which the KUMA agent service is installed. The agent forwards Windows events to KUMA, and you can set up a collector to receive them.

When the agent service is installed, it starts automatically. The service is also configured to restart in case of any failures. The agent can be restarted from the KUMA web interface, but only when the service is active. Otherwise, the service needs to be manually restarted on the Windows asset.

Removing a KUMA agent from Windows assets

To remove a KUMA agent from a Windows asset:

1. Start the Command Prompt on the Windows machine with Administrator privileges and locate the folder with kuma.exe file.

2. Run any of the commands below:

   - `kuma.exe agent --cfg <path to agent configuration file> --uninstall`

   - `kuma.exe agent --id <ID of the agent service that was created in KUMA> --uninstall`

   The specified KUMA agent is removed from the Windows asset. Windows events are no longer sent to KUMA.

When configuring services, you can check the configuration for errors before installation by running the agent with the following command:

```
kuma agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID> --user <user>
```

Update agents

When updating KUMA versions, the WMI, WEC, and ETW agents installed on remote machines must also be updated.

To update the agent, use an administrator account and follow these steps:

1. In Windows, in the **Services** section, open the agent and click **Stop**.

2. On the command line, go to the folder where the agent is installed and run the command to remove the agent from the server.

   ```
   kuma.exe agent --id <agent_ID> --uninstall
   ```

   where:

   <agent_ID> is the ID of the agent service created in KUMA.

3. Place the new agent in the same folder.

4. On the command line, go to the folder with the new agent and from that folder, run the installation command using the agent ID from step 1.

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <agent_ID> --user <user> --install
   ```

   where:

   - <FQDN> is the fully qualified domain name of the KUMA Core server.

   - <port> is the port that the KUMA Core server uses for internal communications (port 7210 is used by default).

   - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

     The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
     You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

     To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

   - <agent_ID> is the ID of the agent service created in KUMA.

   - <user> is the user name of the user that the agent will run as, including the domain.

5. When when installing the updated agent on a device for the first time, you must confirm the license. During the installation process, you are prompted to read the text of the license and then accept or reject the agreement. If this did not happen automatically, you can use the following command to view the text of the license:

   `kuma.exe license --show`

   If you want to accept the license agreement, run the command and press `y`:

   `kuma.exe license`

The agent is updated.

Transferring events from isolated network segments to KUMA

Data transfer scenario

Data diodes can be used to transfer events from isolated network segments to KUMA. Data transfer is organized as follows:

1. KUMA agent that is Installed on a standalone server, with a **diode** destination receives events and moves them to a directory from which the data diode will pick up the events.

   The agent accumulates events in a buffer until it overflows or for a user-defined period after the last write to disk. The events are then written to a file in the temporary directory of the agent. The file is moved to the directory processed by the data diode; its name is a combination of the file contents hash (SHA-256) and the file creation time.

2. The data diode moves files from the isolated server directory to the external server directory.

3. A KUMA collector with a **diode** connector installed on an external server reads and processes events from the files of the directory where the data diode places files.

   After all events are read from a file, it is automatically deleted. Before reading events, the contents of files are verified based on the hash in the file name. If the contents fail verification, the file is deleted.

In the described scenario, the KUMA components are responsible for moving events to a specific directory within the isolated segment and for receiving events from a specific directory in the external network segment. The data diode transfers files containing events from the directory of the isolated network segment to the directory of the external network segment.

For each data source within an isolated network segment, you must create its own KUMA collector and agent, and configure the data diode to work with separate directories.

Configuring KUMA components

Configuring KUMA components for transferring data from isolated network segments consists of the following steps:

1. Creating a collector service in the external network segment.

   At this step, you must create and install a collector to receive and process the files that the data diode will transfer from the isolated network segment. You can use the Collector Installation Wizard to create the collector and all the resources it requires.

   At the **Transport** step, you need to select or create a connector of the **diode** type. In the connector, you must specify the directory to which the data diode will move files from the isolated network segment.

   The user "kuma" that runs the collector must have read/write/delete permissions in the directory to which the data diode moves data from the isolated network segment.

2. Creating a resource set for a KUMA agent.

At this step, you must create a resource set for the KUMA agent that will receive events in an isolated network segment and prepare them for transferring to the data diode. The diode agent resource set has the following requirements:

- The destination in the agent must have the **diode** type. In this resource, you must specify the directory from which the data diode will move files to the external network segment.
- You cannot select connectors of the **sql** or **netflow** types for the diode agent.
- The following **TLS Mode** values are allowed in the diode agent connector: **Disabled**, **Custom PFX**, **Custom PFX with client authentication**. If the **Enabled** is selected, the configuration file cannot be downloaded.

3. Downloading the agent configuration file as JSON file.

   a. The set of agent resources from a diode-type destination must be downloaded as a JSON file.

   b. If secret resources were used in the agent resource set, you must manually add the secret data to the configuration file.

4. Installing the KUMA agent service in the isolated network segment.

   At this step, you must install the agent in an isolated network segment based on the agent configuration file that was created at the previous step. It can be installed to Linux and Windows devices.

Configuring a data diode

The data diode must be configured as follows:

- Data must be transferred atomically from the directory of the isolated server (where the KUMA agent places the data) to the directory of the external server (where the KUMA collector reads the data).
- The transferred files must be deleted from the isolated server.

For information on configuring the data diode, please refer to the documentation for the data diode used in your organization.

Special considerations

When working with isolated network segments, operations with SQL and NetFlow are not supported.

When using the scenario described above, the agent cannot be administered through the KUMA web interface because it resides in an isolated network segment. Such agents are not displayed in the list of active KUMA services.

Diode agent configuration file

A created set of agent resources with a **diode** type destination can be downloaded as a configuration file. This file is used when installing the agent in an isolated network segment.

To download the configuration file:

1. In the web interface, go to the **Resources** → **Agents** section.

2. Select the relevant set of agent resources with the diode destination and click **Download configuration**.

The agent settings configuration is downloaded as a JSON file based on the settings of your browser. Secrets used in the agent resource set are downloaded empty. Their IDs are specified in the file in the `secrets` section. To use a configuration file to install an agent in an isolated network segment, you must manually add secrets to the configuration file (for example, specify the URL and passwords used in the agent connector to receive events).

Using an access control list (ACL) configure permissions to access the file on the server where the agent will be installed. File read access must be available to the user account that will run the diode agent.

Example of a diode agent configuration file with a kafka connector

```
{
    "config": {
        "id": "<ID of the set of agent resources>",
        "name": "<name of the set of agent resources>",
        "proxyConfigs": [
            {
                "connector": {
                    "id": "<ID of the connector>.This example shows a connector of kafka type, but other types of connectors can also be used in a diode agent.If a connector is created directly in the set of agent resources, the ID is not defined.>",
                    "name": "<name of the connector>",
                    "kind": "kafka",
                    "connections": [
                        {
                            "kind": "kafka",
                            "urls": [
                                "localhost:9093"
                            ],
                            "host": "",
                            "port": "",
                            "secretID": "<ID of the secret>",
                            "clusterID": "",
                            "tlsMode": "",
                            "proxy": null,
                            "rps": 0,
                            "maxConns": 0,
                            "urlPolicy": "",
                            "version": "",
                            "identityColumn": "",
                            "identitySeed": "",
                            "pollInterval": 0,
                            "query": "",
                            "stateID": "",
                            "certificateSecretID": "",
                            "authMode": "pfx",
                            "secretTemplateKind": "",
                            "certSecretTemplateKind": ""
                        }
                    ],
                    "topic": "<kafka topic name>",
                    "groupID": "<ID of the kafka group>",
                    "delimiter": "",
                    "bufferSize": 0,
                    "characterEncoding": "",
                    "query": "",
                    "pollInterval": 0,
                    "workers": 0,
                    "compression": "",
                    "debug": false,
                    "logs": [],
                    "defaultSecretID": "",
                    "snmpParameters": [
                        {
                            "name": "",
                            "oid": "",
                            "key": ""
                        }
```

```
                    ],
                    "remoteLogs": null,
                    "defaultSecretTemplateKind": ""
                },
                "destinations": [
                    {
                        "id": "<ID of the destination.If the destination is created directly in the set of agent
resources, the ID is not defined.>",
                        "name": "<destination name>",
                        "kind": "diode",
                        "connection": {
                            "kind": "file",
                            "urls": [
                                "<path to the directory where the destination should place events that the data
diode will transfer from the isolated network segment>",
                                "<path to the temporary directory in which events are placed to prepare for data
transfer by the diode>"
                            ],
                            "host": "",
                            "port": "",
                            "secretID": "",
                            "clusterID": "",
                            "tlsMode": "",
                            "proxy": null,
                            "rps": 0,
                            "maxConns": 0,
                            "urlPolicy": "",
                            "version": "",
                            "identityColumn": "",
                            "identitySeed": "",
                            "pollInterval": 0,
                            "query": "",
                            "stateID": "",
                            "certificateSecretID": "",
                            "authMode": "",
                            "secretTemplateKind": "",
                            "certSecretTemplateKind": ""
                        },
                        "topic": "",
                        "bufferSize": 0,
                        "flushInterval": 0,
                        "diskBufferDisabled": false,
                        "diskBufferSizeLimit": 0,
                        "healthCheckPath": "",
                        "healthCheckTimeout": 0,
                        "healthCheckDisabled": false,
                        "timeout": 0,
                        "workers": 0,
                        "delimiter": "",
                        "debug": false,
                        "disabled": false,
                        "compression": "",
                        "filter": null,
                        "path": ""
                    }
                ]
            }
        ],
        "workers": 0,
        "debug": false
    },
    "secrets": {
        "<ID of the secret>": {
            "pfx": "<encrypted pfx key>",
            "pfxPassword": "<password of the encrypted pfx key.The changeit value is exported from KUMA instead of
the actual password.In the configuration file, you must manually specify the contents of secrets>"
        }
    },
"tenantID": "<ID of the tenant>"
}
```

Description of secret fields

Secret fields

Field name	Type	Description
`user`	string	User name
`password`	string	Password
`token`	string	Token
`urls`	array of strings	URL list
`publicKey`	string	Public key (used in PKI)
`privateKey`	string	Private key (used in PKI)
`pfx`	string containing the base64-encoded pfx file	Base64-encoded contents of the PFX file. In Linux, you can get the base64 encoding of a file by running the following command: `base64 -w0 src > dst`
`pfxPassword`	string	Password of the PFX
`securityLevel`	string	Used in snmp3. Possible values: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`
`community`	string	Used in snmp1
`authProtocol`	string	Used in snmp3. Possible values: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
`privacyProtocol`	string	Used in snmp3. Possible values: `DES`, `AES`
`privacyPassword`	string	Used in snmp3
`certificate`	string containing the base64-encoded pem file	Base64-encoded contents of the PEM file. In Linux, you can get the base64 encoding of a file by running the following command: `base64 -w0 src > dst`

Installing Linux Agent in an isolated network segment

To install a KUMA agent to a Linux device in an isolated network segment:

1. Place the following files on the Linux server in an isolated network segment that will be used by the agent to receive events and from which the data diode will move files to the external network segment:

   - Agent configuration file.

     > You must use an access control list (ACL) to configure access permissions for the configuration file so that only the KUMA user will have file read access.

   - The /opt/kaspersky/kuma/kuma executable file (the `kuma` file can be found inside the installer in the /kuma-ansible-installer/roles/kuma/files/ directory).

2. Execute the following command:

```
sudo ./agent agent --cfg <config_path> --wd <directory_path> --install
```

where:

- <config_path> is the path to the agent configuration file.
- <directory_path> is the path to the directory for the files of the agent that is being installed. If this option is not specified, the files are stored in the directory where the `kuma` file is located.

The agent service is installed and running on the server in an isolated network segment. It receives events and relays them to the data diode so that they can be sent to an external network segment.

Installing Windows Agent in an isolated network segment

Prior to installing a KUMA agent to a Windows asset, the server administrator must create a user account with the EventLogReaders and Log on as a service permissions on the Windows asset. This user account must be used to start the agent.

To install a KUMA agent to a Windows device in an isolated network segment:

1. Place the following files on the Window server in an isolated network segment that will be used by the agent to receive events and from which the data diode will move files to the external network segment:

   - Agent configuration file.

     You must use an access control list (ACL) to configure access permissions for the configuration file so that the file can only be read by the user account that will run the agent.

   - Kuma.exe executable file. This file can be found inside the installer in the /kuma-ansible-installer/roles/kuma/files/ directory.

   We recommend using the `C:\Users\<user name>\Desktop\KUMA` folder.

2. Start the Command Prompt on the Windows asset with Administrator privileges and locate the folder containing the kuma.exe file.

3. Execute the following command:

   ```
   kuma.exe agent --cfg <path to the agent configuration file> --user <user name that will run the agent, including the domain> --install
   ```

   You can get installer Help information by running the following command:

```
kuma.exe help agent
```

4. Enter the password of the user account used to run the agent.

   The `C:\Program Files\Kaspersky Lab\KUMA\agent\<Agent ID>` folder is created in which the KUMA agent service is installed. The agent moves events to the folder so that they can be processed by the data diode.

> When installing the agent, the agent configuration file is moved to the directory C:\Program Files\Kaspersky Lab\KUMA\agent\<agent ID specified in the configuration file>. The kuma.exe file is moved to the C:\Program Files\Kaspersky Lab\KUMA directory.

> When installing an agent, its configuration file must not be located in the directory where the agent is installed.

When the agent service is installed, it starts automatically. The service is also configured to restart in case of any failures.

Removing a KUMA agent from Windows assets

To remove a KUMA agent from a Windows asset:

1. Start the Command Prompt on the Windows machine with Administrator privileges and locate the folder with kuma.exe file.

2. Run any of the commands below:

   - `kuma.exe agent --cfg <path to agent configuration file> --uninstall`

   - `kuma.exe agent --id <ID of the agent service that was created in KUMA> --uninstall`

   The specified KUMA agent is removed from the Windows asset. Windows events are no longer sent to KUMA.

> When configuring services, you can check the configuration for errors before installation by running the agent with the following command:

```
kuma.exe agent --cfg <path to agent configuration file>
```

Configuring an agent to receive NetFlow events from an isolated segment

To receive NetFlow events from an isolated network segment, a dedicated agent installed within this segment is used. The agent acts as an intermediate node: it receives NetFlow events locally and forwards them to the collector where the NetFlow connector is configured.

The transfer of events from the agent to the collector is performed over the UDP protocol.

To configure receiving NetFlow events:

1. Create or configure a collector with a netflow connector and at the **Transport** step, on the **Advanced settings** tab, set **Buffer size** to **65467**.

2. Ensure that the isolated segment allows outbound UDP traffic to the collector.

3. Create an agent for receiving events and configure the sending of events to the collector with the **NetFlow** connector:

   a. In the KUMA web interface, under **Resources and services** → **Agents**, click **Create**.

   b. In the **Create agent** window that opens, on the **Base settings** tab, specify the **Name** and **Tenant** settings.

   c. On the **Configuration resource #{{index}}** tab, under **Connector**, on the **Basic settings** tab, specify the following settings:

      - **Name**—specify the name of the connector.

      - **Type**—specify the **udp** connector type.

      - **URL**—specify the host on which the agent for receiving NetFlow events will be installed.

   d. On the **Configuration resource #{{index}}** tab, under **Connector**, on the **Advanced settings** tab, specify the following settings:

      - Set the **Buffer size** to **65467**. This is the maximum buffer size in bytes.

   e. On the **Configuration resource #{{index}}** tab, under **Destinations**, on the **Basic settings** tab, specify the following settings:

      - **Name**—specify the name of the destination.

      - **Type**—specify the UDP protocol to be used to send events.

      - **URL**—specify the host where the collector with the **NetFlow** connector is installed.

   f. On the **Configuration resource #{{index}}** tab, under **Destinations**, on the **Advanced settings** tab, specify the following settings:

      - Set the **Buffer size** to **65467**. This is the maximum buffer size in bytes.

   g. Click **Create**.

   h. Install the agent in the isolated network segment. It can be installed to Linux and Windows devices.

Receiving NetFlow events from the isolated segment is configured.

Getting service data about events from an isolated segment

Service data about events is transmitted to the collector via the 'internal' protocol. To transfer such data from an isolated network segment, you can use a dedicated agent installed within this segment.

To transfer data from the agent to the collector via the 'internal' protocol, the agent and the collector must authenticate each other using certificates. You can create and save the agent certificate in the agent's configuration file and then use this file to install the agent in the isolated segment. Certificate information is saved in the file in an encrypted form.

To configure the receipt of service data about events from an isolated segment:

1. Create or configure a collector with the 'internal' connector.

2. Create an agent and configure data transmission to the collector:

   a. In the KUMA web interface, under **Resources and services** → **Agents**, click **Create**.

   b. In the **Create agent** window that opens, on the **Base settings** tab, specify the **Name** and **Tenant** settings.

   c. On the **Configuration resource #{{index}}**, in the **Connector** section, specify the following settings:

      - In the **Name** field, specify the name of the connector.
      - In the **Type** field, specify the connector type.
      - In the **URL** field, specify the host on which the agent for receiving events will be installed.

   d. On the **Configuration resource #{{index}}**, in the **Destinations** section, specify the following settings:

      - In the **Name** field, specify the name of the destination.
      - In the **Type** field, enter the **internal** protocol that will be used to send events.
      - In the **URL** field, specify the host on which the collector with the **internal** connector is installed.

   e. Click **Create**.

   f. Select the created resource set of the agent from the list, then in the agent properties window, click **Download the configuration containing the certificate**. In the displayed window, specify the password that will be used to encrypt the certificate, and will also be requested when starting the agent.

      The agent settings configuration is downloaded as a JSON file based on the settings of your browser. This file is used when installing the agent in an isolated network segment.

      > You must use an access control list (ACL) to configure permissions to access the file on the server where the agent will be installed. File read access must be available to the user account that the agent will run as.

   g. Install the agent in the isolated network segment. It can be installed to Linux and Windows devices.

Receipt of service data about events from an isolated segment is configured.

Receiving sensitive data over an encrypted connection

Event sources transmit data over the network without encryption. If the data contains sensitive information, the transmission of such data over the network as clear text cannot be allowed to occur.

In KUMA, you can use an agent to transmit data from a source to a collector over an encrypted connection. In this case, the method of transmitting data from the source to the agent depends on where the agent is installed.

The following methods are available:

- Receiving data via the 'internal' protocol.

  The KUMA agent is installed on the same host as the event source. The event source passes data to the agent locally as a file, and the agent transmits it to the collector via the 'internal' protocol.

- Receiving data using a protocol with TLS encryption support.

  The KUMA agent is installed in an isolated network segment, not necessarily on the same host as the event source. The event source transmits data to the agent via UDP in the form of data packets, and the agent transmits the data it received to the collector using a protocol that supports TLS encryption. In this case, unencrypted UDP transmission is restricted to the isolated network segment, and agent-to-collector communication is encrypted.

Receiving data via the 'internal' protocol

In the following example data retrieval configuration, the KUMA agent is installed on the same host as the source. The agent receives events from the event source and passes them to the collector as a file using the 'internal' protocol. You can adapt this example to suit your requirements.

To configure the receipt of events via the 'internal' protocol:

1. Create or configure a collector and at the **Transport** step, on the **Advanced settings** tab, set **Buffer size** to **65467**.

2. Create an agent for receiving events and configure the sending of events to the collector using the 'internal' protocol:

   a. In the KUMA web interface, under **Resources and services** → **Agents**, click **Create**.

   b. In the **Create agent** window that opens, on the **Base settings** tab, specify the **Name** and **Tenant** settings.

   c. Open the **Configuration resource #{{index}}**.

   d. Under **Connector**, specify the following:

      1. On the **Basic settings** tab:

         - In the **Name** field, specify the name of the connector.

         - In the **Type** field, specify the **file** type.

         - In the **File path** field, specify the full path to the log file.

      2. On the **Advanced settings** tab, in the **Buffer size field**, enter **65467**.

         This is the maximum buffer size in bytes.

e. Under **Destinations**, specify the following:

1. On the **Basic settings** tab:

   - In the **Name** field, specify the name of the destination.
   - In the **Type** field, enter the **internal** protocol that will be used to send events.
   - In the **URL** field, specify the host on which the collector for data will be installed.

2. On the **Advanced settings** tab, in the **Buffer size field**, enter **65467**.

   This is the maximum buffer size in bytes.

f. Click **Create**.

g. Install the agent on the same host as the event source. It can be installed to Linux and Windows devices.

Reception of events over the 'internal' protocol is configured.

Receiving data using a protocol with TLS encryption support

In the following example data retrieval configuration, the KUMA agent is installed on a separate host, not necessarily the same host as the source. The agent receives data from the event source in the isolated segment and transmits the data to the collector using a protocol with TLS encryption. You can adapt this example to suit your requirements.

To configure the receipt of data using a protocol with TLS encryption support:

1. Create or configure a collector and at the **Transport** step, on the **Advanced settings** tab, set **Buffer size** to **65467**.

2. Create an agent for receiving events and configure the sending of events to the collector using a protocol that supports TLS encryption:

   a. In the KUMA web interface, under **Resources and services** → **Agents**, click **Create**.

   b. In the **Create agent** window that opens, on the **Base settings** tab, specify the **Name** and **Tenant** settings.

   c. Open the **Configuration resource #{{index}}**.

   d. Under **Connector**, specify the following:

      1. On the **Basic settings** tab:

         - In the **Name** field, specify the name of the connector.
         - In the **Type** field, specify **udp**.
         - In the **URL** field, specify the host on which the agent for receiving events will be installed.

      2. On the **Advanced settings** tab, in the **Buffer size field**, enter **65467**.

         This is the maximum buffer size in bytes.

e. Under **Destinations**, specify the following:

1. On the **Basic settings** tab:

   - In the **Name** field, specify the name of the destination.
   - **Type**—specify the protocol to be used to send events. You can specify any protocol that supports TLS encryption.
   - In the **URL** field, specify the host on which the collector is installed.

2. On the **Advanced settings** tab:

   - Set the **Buffer size** to **65467**. This is the maximum buffer size in bytes.
   - In the **TLS mode** drop-down list, select **Enabled**.

f. Click **Create**.

g. Install the agent in the isolated network segment. It can be installed to Linux and Windows devices.

Receipt of events using a protocol that supports TLS encryption is now complete.

Transferring events from Windows computers to KUMA

To transfer events from Windows computers to KUMA, a KUMA agent and a KUMA collector are used. Data transfer is performed as follows:

1. The KUMA agent installed on the computer receives Windows events using one of the connectors:

   - WEC. The agent receives events arriving at the host under a subscription, as well as the server logs.
   - WMI. The agent connects to remote servers specified in the configuration and receives events.
   - ETW. The agent connect to the DNS server using the session name and provider specified in the connector settings, and receives events.

2. The agent sends events (without preprocessing) to the KUMA collector specified in the destination.

   You can configure the agent so that different logs are sent to different collectors.

3. The collector receives events from the agent, performs a full event processing cycle, and sends the processed events to the destination.

About using agents

We recommend configuring the receipt of events from Windows devices using the KUMA Agent (WEC) when using centralized collection of events from Windows hosts using the Windows Event Forwarding (WEF) technology (for details about Windows Event Forwarding, see the official Microsoft documentation). The agent must be installed on the server that collects events; it acts as the Windows Event Collector (WEC). We do not recommend installing KUMA agents on every endpoint host from which you want to receive events.

We recommend configuring the receipt of events using a KUMA Agent (WMI) in the following cases:

- The WEF technology cannot be used to implement a centralized collection of events, and installing third-party software (such as the KUMA Agent) on the event source server is prohibited.
- You need to obtain events from a small number of hosts (no more than 500 hosts per one KUMA agent).

The ETW agent is used only to retrieve events from Windows logs of DNS servers.

For connecting Windows logs as an event source, we recommend using the **Add event source** Wizard. When using a wizard to create a collector with WEC or WMI connectors, agents are automatically created for receiving Windows events. You can also manually create the resources necessary for collecting Windows events.

Creating and installing a KUMA agent and collector.

Creating and installing an agent and a collector for receiving Windows events involves the following steps:

1. **Creating a set of resources for an agent.**

   Agent connector:

   When creating an agent, on the **Connection** tab, create or select a connector of the WEC, WMI, or ETW type.

   If at least one Windows log name in a WEC or WMI connector is specified incorrectly, or the WMI server is unavailable, the agent will receive events from all Windows logs listed in the connector, except the problematic log. At the same time the agent status will be green. Attempts to receive events will be repeated every 60 seconds, and error messages will be added to the service log.

   Agent destination:

   The type of agent destination depends on the data transfer method you use: `nats-jetstream`, `tcp`, `http`, `diode`, `kafka`, `file`.

   Use `\0` as the destination separator.

   The advanced settings for the agent destination (such as separator, compression and TLS mode) must match the advanced destination settings for the collector connector that you want to link to the agent.

2. **Creating an agent service in the KUMA web interface**

3. **Installing the KUMA agent on the Windows computer from which you want to receive Windows events.**

   Before installation, make sure that the system components have access to the network and open the necessary network ports:

   - Port 7210, TCP: from the server with collectors to the Core.
   - Port 7210, TCP: from the agent server to the Core.
   - The port specified in the **URL** field when the connector was created: from the agent server to the server with the collector.

4. **Creating and installing a KUMA collector.**

   When creating a set of collector resources, create or select a connector that the collector will use to receive events from the agent at the **Transport** step. Connector type must match the type of the agent destination.

   The advanced settings of the connector (such as delimiter, compression, and TLS mode) must match the advanced settings of the agent destination that you want to link to the agent.

Useful articles

Access is denied error

Events are not being received via the WMI agent

Importing a file with a list of servers for WMI agents

If you have many servers, you can import a .TSV file with a list of event sources for WMI agents so that you do not have to manually fill in the **Server**, **Domain**, and **Log type** settings for the WMI agent for each server. In such a file, you can prepare a list of servers to which the WMI agent will connect and a list of logs that you want to receive from the specified servers.

Requirements for the file with a list of servers for WMI agents.

Acceptable file format: TSV.

If you change the recommended format to **All files** and upload a file that does not comply with the required format (for example, a JSON file, XML file, or some different format instead of TSV), such a file may be parsed incorrectly.

The maximum number of lines in a file with host settings is 500.

The following fields are required:

- **Server** is the name of the host from which the agent will receive logs. Acceptable format: hostname or IP address. Acceptable values: IPv4, IPv6, host name.
- **Domain** is the host ID, for communication with the host over the network. Acceptable format: fully qualified domain name or IP address. Acceptable values: IPv4, IPv6, FQDN.
- **Log type** is a list of logs and/or Windows subscriptions that the agent will receive. Acceptable format: array of strings. For example, you can specify Application, ForwardedEvents, or Security. If the file specifies a value that was not previously present in the list of logs, the log or subscription must be created that will also appear in the list of available for processing using the Windows agent.

  The maximum length of a log value is 1024 characters. You must specify at least one log or subscription.

After importing and filling in all the fields of the remote hosts, a check is performed when you save settings. If any errors are found in the fields, the settings are not saved, and the errors are highlighted. You can manually update the fields as necessary and save the settings.

To import a file with a list of sources:

1. In the **Resources** → **Agents** section of the KUMA interface, create a WMI agent or open the WMI agent settings for editing.
2. This opens a window; in that window, on the **Configuration resource #** tab, in the **Connector** section, specify the name of the connector, in the **Type** drop-down list, select **wmi** and click the **Import TSV** button.
3. This opens a window; in that window, select the prepared file with the list of sources in the .TSV format.

   KUMA parses the file and fills in under **Remote hosts**, fills the **Server**, **Domain**, **Log type** required fields.

4. If necessary, in the **Secret** drop-down list, select a secret of the **Credentials** type or create a secret of the **Credentials** type.

   When importing a list of hosts from a file, in the **Secret** drop-down list, **Default** remains selected, and the agent uses the default credentials when communicating with the server to retrieve logs.

5. If you want to cancel the import of data from the file, click **Cancel**. If you want to delete some data lines imported from a file, in the user interface, select the lines you want to delete and click **Delete**.

6. Save settings in one of the following ways:

   - For a newly created agent, click **Create**. The service is created in the KUMA web interface.

   - For an active agent opened for editing, click **Save**.

7. Apply the saved settings in one of the following ways:

   - For a newly created agent, install the agent service in the KUMA network infrastructure.

   - For an active agent service opened for editing, restart the agent service.

The file with a list of servers for WMI agents is imported.

Managing assets

Assets represent devices and systems in the organization for which security events are received. These systems and devices can include workstations, servers, network equipment, mobile devices, and other infrastructure objects. Assets generate network traffic when they send and receive data. KUMA can be configured to track this activity and create base events with a clear indication of where the traffic is coming from and where it is going. The event can contain source and destination IP addresses, as well as DNS names. If you register an asset with certain parameters (for example, a specific IP address), this asset is linked to all events that mention these parameters (for example, the IP address).

We recommend registering assets in KUMA because using assets allows formulating clear and versatile correlation rules, which makes event analysis more efficient.

After you add assets to KUMA, their IDs are added when enriching events. When analyzing events, you get additional information about the devices and systems in your organization.

You can view information about assets, search for assets by specified criteria, edit or delete assets, and export asset data to a CSV file.

Asset categories

You can group assets by category. This helps keep your network structure transparent and gives you additional ways to work with correlation rules. For example, you can create alerts of a higher severity level for assets from a higher-severity category. By default, all assets fall into the **Uncategorized assets** category. A device can be added to multiple categories.

When an event linked to an asset is processed, the category of this asset is also taken into consideration. For example, if you assign a high severity value to a certain asset category, base events involving these assets will create correlation events with higher severity. This leads into higher-severity alerts and, therefore, a more rapid response to such an alert.

By default, KUMA asset categories have the following severity levels: Low, Medium, High, Critical. You can create custom categories, categories can be nested.

Categories can be populated in the following ways:

- **Manually**
- **Active**: dynamic, if the asset meets the conditions.

  Active filling conditions

  1. In the **Repeat categorization every** drop-down list, specify how often assets will be linked to a category. You can select values ranging from once per hour to once per 24 hours.

     You can forcibly start categorization by selecting **Start categorization** in the category context menu.

  2. Under **Conditions**, specify the filter for matching assets to attach to an asset category.

     You can add conditions by clicking the **Add condition** buttons. Groups of conditions can be added by using the **Add group** buttons. Group operators can be switched between **AND**, **OR**, and **NOT** values.

     Categorization filter operands and operators

Operand	Operators	Comment
Build number	=, ilike	
OS	=, ilike	The **ilike** operator makes the search case-insensitive.
IP address	inSubnet, inRange	The IP address is indicated in CIDR notation (for example: 192.168.0.0/24). When the inRange operator is selected, you can indicate only addresses from private ranges of IP addresses (for example: 10.0.0.0–10.255.255.255). Both addresses must be in the same range.
FQDN	=, ilike	The **ilike** operator makes the search case-insensitive.
CVE	=, in	The **in** operator lets you specify an array of CVE (Common Vulnerabilities and Exposures) IDs, for example, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Severity level of CVE vulnerabilities on the asset. The CVSS parameter takes values from 0 to 10. Not applicable to vulnerabilities from Kaspersky Security Center.

CVE count	>, >=, =, <=, <	The number of unique vulnerabilities with the CVE attribute for the asset. Vulnerabilities without CVEs do not count towards this figure.
		For categorization by the number of CVEs of a certain severity level, you can use a combined condition. For example:
		`CVE count >= 1`
		`AND`
		`CVSS >= 6.5`

Software	=, ilike	Categorization by software installed on the asset. The **ilike** operator makes the search case-insensitive.
Software version	=, ilike, in	Categorization by version (build) number of the software installed on the asset. The **ilike** operator makes the search case-insensitive.
CII	in	More than one value can be selected.
KSC group	=, ilike	Categorization by the name of the Kaspersky Security Center administration group in which the asset is placed.

Anti-virus databases last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is current at the time when categorization is started.
Last update of the information	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Protection last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
System last started	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
KSC extended status	in	Extended status of the device. More than one value can be selected.
Real-time protection status	=	Status of Kaspersky applications installed on the managed device.
Encryption status	=	
Spam protection status	=	
Anti-virus protection status of mail servers	=	
Data Leakage Prevention status	=	
KSC extended status ID	=	
Endpoint Sensor status	=	

Last visible	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Score ML	>,>=,=,<=,<	Categorization by asset score assigned by AI services.
Status	=, in	Categorization by predefined asset statuses assigned by AI services.
Custom asset field	=, ilike	Categorization by values of custom asset fields.

Using time values

Some conditions, for example, **Anti-virus databases last updated** or **System last started**, use date and time as the operand value. For these conditions, you can use an exact date and time or a relative period.

To specify a date and time value:

1. Select an operand, an operator and click the date field.

2. Do one of the following:

   - Select the exact date in the calendar.

     By default, the current time is automatically added to the selected date, with millisecond precision. Changing the date in the calendar does not change the specified time. The date and time are displayed in the time zone of the browser. If necessary, you can edit the date and time in the field.

   - In the **Relative period** list, select a relative period.

     The period is calculated relative to the start time of the current categorization and takes into account asset information that is up-to-date at that moment. For example, for the condition **Anti-virus databases last updated**, you can select **1 hour** and the **>=** operator to periodically link to the category those assets for which the anti-virus databases have not been updated for more than 1 hour before the start of categorization.

   - In the date and time field, enter a value manually.

     You can enter an exact date and time in the **DD.MM.YYYY HH:mm:ss.SSS** format for the Russian localization and **YYYY-MM-DD HH:mm:ss.SSS** for the English localization or a relative period as a formula. You can also combine these methods if necessary.

     If you do not specify milliseconds when entering the exact date, 000 is substituted automatically.

     In the relative period formulas, you can use the **now** parameter for the current date and time and the interval parameterization language: **+**, **-**, **/** (rounding to the nearest), as well as time units: **y** (year), **M** (month), **w** (week), **d** (day), **h** (hour), **m** (minute), **s** (second).

     For example, for the **Information last updated** condition, you can specify the value **now-2d** with the operator **>=** operator and the value **now-1d** with the **>=** operator to regularly link assets to the category if those assets had information updated during the day before the categorization was started; alternatively, you can specify the value **now/w** with the **<=** operator to regularly link assets to the category if those assets had information updated between the beginning of the first day of the current week (00:00:00:000 UTC) and **now**.

KUMA stores time values in UTC, but in the user interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the period, the category will cover assets from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the date and time field by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want the categorization to cover the **Yesterday** period, you need to change the value to **now-1d/d-3h**. If you want the categorization to cover the **Today** period, change the value to **now/d-3h**.

3. Use the **Test conditions** button to make sure that the specified filter is correct. When you click the button, the **Assets for given conditions** window containing a list of assets that satisfy the search conditions will be displayed.

For example, the moment the asset is upgraded to a specified OS version or placed in a specified subnet, the asset is moved to the specified category. If you specified a relative period and selected the frequency of categorization, for example, hourly, every time categorization starts, the condition will consider asset information that is up-to-date at the time of starting the categorization.

- **Reactive**—When a correlation rule is triggered, the asset is moved to the specified group.

In KUMA, assets are categorized by tenant and by category. Assets are arranged in a tree structure, where the tenants are located at the root, and the asset categories branch from them. You can view the tree of tenants and categories in the **Assets** → **All assets** section of the KUMA web interface. When a tree node is selected, the assets assigned to it are displayed in the right part of the window. Assets from the subcategories of the selected category are displayed if you specify that you want to display assets recursively. You can select the check boxes next to the tenants whose assets you want to view.

To open the context menu of a category, hover the mouse cursor over the category and click the ellipsis icon that is displayed to the right of the category name. The following actions are available in the context menu:

Category context menu items

Action	Description
Show assets	Display assets of the selected category in the right part of the window.
Show assets recursively	View assets from subcategories of the selected category. If you want to exit recursive viewing mode, select another category to view.
Show info	View information about the selected category in the **Category information** details area displayed in the right part of the web interface window.
Start categorization	Start automatic update of assets in the selected category. During the update, new assets can be linked or previously linked assets can be unlinked. This option is available for categories that have active categorization.
Add subcategory	Add a subcategory to the selected category.
Edit category	Edit the selected category.
Delete category	Delete the selected category. You can only delete categories that have no assets or subcategories. Otherwise the **Delete category** option is inactive.
Pin as tab	Display the selected category on a separate tab. You can undo this action by selecting **Unpin as tab** in the context menu of the relevant category.

Adding an asset category

To add an asset category:

1. Open the **Assets** section in the KUMA web interface.

2. Open the category creation window by doing the following:

   a. In the list of tenants, expand the tenant to which you want to add the new category.

   b. Hover over the parent category and do one of the following:

      - Click the plus (+) icon.

      - In the menu (⋮) select **Add subcategory**.

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

3. Add information about the category:

   - In the **Name** field, enter the name of the category. The name must contain 1 to 128 Unicode characters.

   - If necessary, change the category in the **Parent** drop-down list.

   - The **Tenant** field displays the tenant in whose structure you selected the parent category. You cannot change the previously selected tenant.

   - If necessary, change the severity of the category in the **Severity** drop-down list. The default value is **Low**.

   - If necessary, in the **Description** field, you can add a note consisting of up to 4000 Unicode characters.

4. In the **Categorization kind** drop-down list, select how the category will be populated with assets. Depending on your selection, you may need to specify additional settings:

   - **Manually**—assets can only be manually linked to a category.

   - **Active**—assets are periodically assigned to a category if they satisfy the specified condition. If an asset no longer satisfies this condition, such an asset is unlinked from the category, regardless of whether the assets were added automatically or manually.

     Active category of assets

     1. In the **Repeat categorization every** drop-down list, specify how often assets will be linked to a category. You can select values ranging from once per hour to once per 24 hours.

        You can forcibly start categorization by selecting **Start categorization** in the category context menu.

     2. Under **Conditions**, specify the filter for matching assets to attach to an asset category.

        You can add conditions by clicking the **Add condition** buttons. Groups of conditions can be added by using the **Add group** buttons. Group operators can be switched between **AND**, **OR**, and **NOT** values.

        Categorization filter operands and operators

Operand	Operators	Comment
Build number	=, ilike	
OS	=, ilike	The **ilike** operator makes the search case-insensitive.
IP address	inSubnet, inRange	The IP address is indicated in CIDR notation (for example: 192.168.0.0/24). When the inRange operator is selected, you can indicate only addresses from private ranges of IP addresses (for example: 10.0.0.0–10.255.255.255). Both addresses must be in the same range.
FQDN	=, ilike	The **ilike** operator makes the search case-insensitive.
CVE	=, in	The **in** operator lets you specify an array of CVE (Common Vulnerabilities and Exposures) IDs, for example, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Severity level of CVE vulnerabilities on the asset. The CVSS parameter takes values from 0 to 10. Not applicable to vulnerabilities from Kaspersky Security Center.

CVE count	>, >=, =, <=, <	The number of unique vulnerabilities with the CVE attribute for the asset. Vulnerabilities without CVEs do not count towards this figure.
		For categorization by the number of CVEs of a certain severity level, you can use a combined condition. For example:
		`CVE count >= 1`
		`AND`
		`CVSS >= 6.5`

Software	=, ilike	Categorization by software installed on the asset. The **ilike** operator makes the search case-insensitive.
Software version	=, ilike, in	Categorization by version (build) number of the software installed on the asset. The **ilike** operator makes the search case-insensitive.
CII	in	More than one value can be selected.
KSC group	=, ilike	Categorization by the name of the Kaspersky Security Center administration group in which the asset is placed.
Anti-virus databases last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is current at the time when categorization is started.
Last update of the information	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Protection last updated	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.

System last started	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
KSC extended status	in	Extended status of the device. More than one value can be selected.
Real-time protection status	=	Status of Kaspersky applications installed on the managed device.
Encryption status	=	
Spam protection status	=	
Anti-virus protection status of mail servers	=	
Data Leakage Prevention status	=	
KSC extended status ID	=	
Endpoint Sensor status	=	
Last visible	>=,<=	For categorization, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below. A relative period for repeated categorization takes into account asset information that is up-to-date at the time when categorization is started.
Score ML	>,>=,=,<=,<	Categorization by asset score assigned by AI services.
Status	=, in	Categorization by predefined asset statuses assigned by AI services.
Custom asset field	=, ilike	Categorization by values of custom asset fields.

Using time values

Some conditions, for example, **Anti-virus databases last updated** or **System last started**, use date and time as the operand value. For these conditions, you can use an exact date and time or a relative period.

To specify a date and time value:

1. Select an operand, an operator and click the date field.

2. Do one of the following:

   - Select the exact date in the calendar.

     By default, the current time is automatically added to the selected date, with millisecond precision. Changing the date in the calendar does not change the specified time. The date and time are displayed in the time zone of the browser. If necessary, you can edit the date and time in the field.

- In the **Relative period** list, select a relative period.

  The period is calculated relative to the start time of the current categorization and takes into account asset information that is up-to-date at that moment. For example, for the condition **Anti-virus databases last updated**, you can select **1 hour** and the **>=** operator to periodically link to the category those assets for which the anti-virus databases have not been updated for more than 1 hour before the start of categorization.

- In the date and time field, enter a value manually.

  You can enter an exact date and time in the **DD.MM.YYYY HH:mm:ss.SSS** format for the Russian localization and **YYYY-MM-DD HH:mm:ss.SSS** for the English localization or a relative period as a formula. You can also combine these methods if necessary.

  If you do not specify milliseconds when entering the exact date, 000 is substituted automatically.

  In the relative period formulas, you can use the **now** parameter for the current date and time and the interval parameterization language: **+**, **-**, **/** (rounding to the nearest), as well as time units: **y** (year), **M** (month), **w** (week), **d** (day), **h** (hour), **m** (minute), **s** (second).

  For example, for the **Information last updated** condition, you can specify the value **now-2d** with the operator **>=** operator and the value **now-1d** with the **>=** operator to regularly link assets to the category if those assets had information updated during the day before the categorization was started; alternatively, you can specify the value **now/w** with the **<=** operator to regularly link assets to the category if those assets had information updated between the beginning of the first day of the current week (00:00:00:000 UTC) and **now**.

  KUMA stores time values in UTC, but in the user interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the period, the category will cover assets from 03:00:00.000 until now, not from 00:00:00.000 until now.

  If you want to take your time zone into account when selecting a relative period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the date and time field by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want the categorization to cover the **Yesterday** period, you need to change the value to **now-1d/d-3h**. If you want the categorization to cover the **Today** period, change the value to **now/d-3h**.

3. Use the **Test conditions** button to make sure that the specified filter is correct. When you click the button, the **Assets for given conditions** window containing a list of assets that satisfy the search conditions will be displayed.

- **Reactive**—the category will be filled with assets by using correlation rules.

5. Click **Save**.

The new category will be added to the asset categories tree.

Configuring the table of assets

In KUMA, you can configure the contents and order of columns displayed in the assets table. These settings are stored locally on your machine.

To configure the settings for displaying the assets table:

1. Open the **Assets** section in the KUMA web interface.

2. Click the gear (⚙) icon in the upper-right corner of the assets table.

3. In the drop-down list, select the check boxes next to the parameters that you want to view in the table:

   - **FQDN**
   - **IP address**
   - **Asset source**
   - **Owner**
   - **MAC address**
   - **Created by**
   - **Updated**
   - **Tenant**
   - **CII category**
   - **Archived**
   - **Status**
   - **Score ML**

   When you select a check box, the assets table is updated and a new column is added. When a check box is cleared, the column disappears. The table can be sorted based on multiple columns.

4. If you need to change the order of columns, click the left mouse button on the column name and drag it to the desired location in the table.

The assets table display settings are configured.

Searching assets

KUMA has two asset search modes. You can switch between the search modes using the buttons in the upper left part of the window:

- – simple search by the following asset settings: **Name**, **FQDN**, **IP address**, **MAC address**, and **Owner**.
- – advanced search for assets using filters by conditions and condition groups.

You can select the check boxes next to the found assets to export their data to a CSV file.

Simple search

To find an asset using simple search:

1. In the **Assets** section of the KUMA web interface, click the button.

   The **Search** field is displayed at the top of the window.

2. Enter your search query in the **Search** field and press **ENTER** or click the icon.

The table displays the assets with the **Name**, **FQDN**, **IP address**, **MAC address**, and **Owner** settings matching the search criteria.

Advanced search

To find an asset using advanced search:

1. In the **Assets** section of the KUMA web interface, click the button.

   The asset filtering settings are displayed in the upper part of the window.

2. Specify the asset filtering settings and click the **Search** button.

   For details on asset filtering settings, see the table below.

The table displays the assets that meet the search criteria.

An advanced asset search is performed using the filtering conditions that can be specified in the upper part of the window:

- You can use the **Add condition** button to add a string containing fields for identifying the condition.
- You can use the **Add group** button to add a group of filters. Group operators can be switched between **AND**, **OR**, and **NOT**.
- Conditions and condition groups can be dragged with the mouse.
- Conditions, groups, and filters can be deleted by using the button.
- You can collapse the filtering options by clicking the **Collapse** button. In this case, the resulting search expression is displayed. Clicking it displays the search criteria in full again.
- The filtering options can be reset by clicking the **Clear** button.
- The condition operators and available values of the right operand depend on the selected left operand:

Left operand	Available operators	Right operand
Build number	=, ilike	An arbitrary value.
OS	=, ilike	An arbitrary value.

Left operand	Available operators	Right operand
IP address	inSubnet, inRange	An arbitrary value or a range of values. The filtering condition for the inSubnet operator is met if the IP address in the left operand is included in the subnet that is specified in the right operand. For example, the subnet for the IP address 10.80.16.206 should be specified in the right operand using slash notation as follows: `10.80.16.206/25`.
FQDN	=, ilike	An arbitrary value.
CVE	=, in	An arbitrary value. The **in** operator lets you specify an array of CVE (Common Vulnerabilities and Exposures) IDs, for example, `CVE-2017-0143`.
CVSS	>, >=, =, <=, <	A number from 0 to 10 (possible severity levels of the asset's CVE vulnerability). Not applicable to vulnerabilities from Kaspersky Security Center.

CVE count	>, >=, =, <=, <	Number. The number of unique vulnerabilities with the CVE attribute for the asset. Vulnerabilities without CVEs do not count towards this figure.
		If `0` is specified as the right operand and the `=` or `<=` operator is selected, the search results include assets that do not have CVE vulnerabilities.
		For searching by the number of CVEs of a certain severity level, you can use a combined condition. For example:
		`CVE count >= 1`
		`CVSS >= 6.5`

Software	=, ilike	An arbitrary value.
Software version	=, ilike, in	An arbitrary value. Version (build) number of the software installed on the asset.
Asset source	in	• Kaspersky Security Center. • KICS/KATA. • Created manually
CII	in	• Information resource is not a CII object. • CII object without a significance category. • CII object of the third category of significance. • CII object of the second category of significance. • CII object of the first category of significance.
RAM (bytes)	=, >, >=, <, <=	Number.
Number of disks	=, >, >=, <, <=	Number.
Number of network cards	=, >, >=, <, <=	Number.
Disk free bytes	=, >, >=, <, <=	Number.
KSC group	=, ilike	An arbitrary value. Name of the Kaspersky Security Center administration group in which the asset is placed.
Anti-virus databases last updated	>=, <=	For searching, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below.
Last update of the information	>=, <=	For searching, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below.

Left operand	Available operators	Right operand
Protection last updated	>=, <=	For searching, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below.

Left operand	Available operators	Right operand
System last started	>=, <=	For searching, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below.
KSC extended status	in	• Host with Network Agent installed is online, but Network Agent is inactive. • Anti-virus application is installed, but real-time protection is not running. • Anti-virus application is installed but not running. • Number of viruses detected is too high. • Anti-virus application is installed but the real-time protection status differs from the one set by the security administrator. • Anti-virus application is not installed. • Full scan for viruses performed too long ago. • Anti-virus bases were updated too long ago. • Network Agent has been inactive too long. • Old license. • Number of uncured objects is too high. • Reboot is required. • One or more incompatible applications are installed on the host. • Host has one or more vulnerabilities. • Last search for operating system updates was performed too long ago on the host. • The host does not have the proper encryption status. • Mobile device settings do not meet the requirements of the security policy. • There are unhandled incidents. • Host status was suggested by the managed product (HSDP). • Host is out of disk space, either synchronization errors occur, or disk space is running out.
Real-time protection status	=	• Unknown. • Stopped. • Suspended. • Starting. • Running (if anti-virus application does not support categories of state Running). • Running with maximum protection. • Running for maximum speed. • Running with recommended settings. • Running with custom settings. • Error.
Encryption status	=	• Encryption rules are not configured on the host. • Encryption is in progress. • Encryption was canceled by the user. • Encryption error occurred. • All host encryption rules are met. • Encryption is in progress, the host must be restarted. • Encrypted files without specified encryption rules are detected on the host.
Spam protection status	=	• Unknown. • Stopped. • Suspended. • Starting. • Running. • Error. • Not installed. • No license.
Anti-virus protection status of mail servers	=	• Unknown. • Stopped. • Suspended. • Starting. • Running. • Error. • Not installed. • No license.
Data Leakage Prevention status	=	• Unknown. • Stopped. • Suspended. • Starting. • Running. • Error. • Not installed. • No license.

Left operand	Available operators	Right operand
KSC extended status ID	=	• OK • Critical. • Warning.
Endpoint Sensor status	=	• Unknown. • Stopped. • Suspended. • Starting. • Running. • Error. • Not installed. • No license.
Last visible	>=, <=	For searching, the time is specified as UTC time, and then converted in the KUMA interface to the local time zone set in the browser. You can specify the date and time for this operand in one of the following ways: • Select the exact date in the calendar. • Select a period relative to the present time in the **Relative period** list. • Enter a value manually: an exact date and time or a relative period, or a combination of both. For details, check the *Using time values* subsection below.
Score ML	=, >, >=, <, <=	Number. Asset score assigned by AI services.
Status	=, in	Asset status assigned by AI services: • Low. • Medium. • High. • Critical.
Custom asset field	=, ilike	An arbitrary value. Search custom fields of assets.

Using time values

Some conditions, for example, **Anti-virus databases last updated** or **System last started**, use date and time as the operand value. For these conditions, you can use an exact date and time or a relative period.

To specify a date and time value:

1. Select an operand, an operator and click the date field.

2. Do one of the following:

   - Select the exact date in the calendar.

     By default, the current time is automatically added to the selected date, with millisecond precision. Changing the date in the calendar does not change the specified time. The date and time are displayed in the time zone of the browser. If necessary, you can edit the date and time in the field.

   - In the **Relative period** list, select a relative period.

     The period is calculated relative to the start time of the current search and takes into account asset information that is up-to-date at that moment. For example, for the condition **Anti-virus databases last updated**, you can select **1 hour** and the **>=** operator to find those assets for which the anti-virus databases have not been updated for more than 1 hour.

   - In the date and time field, enter a value manually.

     You can enter an exact date and time in the **DD.MM.YYYY HH:mm:ss.SSS** format for the Russian localization and **YYYY-MM-DD HH:mm:ss.SSS** for the English localization or a relative period as a formula. You can also combine these methods if necessary.

If you do not specify milliseconds when entering the exact date, 000 is substituted automatically.

In the relative period formulas, you can use the **now** parameter for the current date and time and the interval parameterization language: **+**, **-**, **/** (rounding to the nearest), as well as time units: **y** (year), **M** (month), **w** (week), **d** (day), **h** (hour), **m** (minute), **s** (second).

For example, for the **Information last updated** condition, you can specify **now-2d** with the **>=** operator and **now-1d** with the **>=** operator to find assets whose information was last updated the day before the search was started; or you can specify **now/w** with the **<=** operator to find assets whose information was last updated between the start of the first day of the current week (00:00:00:000 UTC) and the current time, **now**.

KUMA stores time values in UTC, but in the user interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the period, the category will cover assets from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the date and time field by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want the categorization to cover the **Yesterday** period, you need to change the value to **now-1d/d-3h**. If you want the categorization to cover the **Today** period, change the value to **now/d-3h**.

Exporting asset data

You can export data about the assets displayed in the assets table as a CSV file.

To export asset data:

1. Configure the assets table.

   Only the data specified in the table is written to the file. The display order of the asset table columns is preserved in the exported file.

2. Find the desired assets and select the check boxes next to them.

   You can select all the assets in the table at a time by selecting the check box in the left part of the assets table header.

3. Click the **Export CSV** button.

The asset data is written to the assets_<export date>_<export time>.csv file. The file is downloaded according to your browser settings.

Viewing asset details

To view information about an asset, open the asset information window in one of the following ways:

- In the KUMA web interface, select **Assets** → select a category with the relevant assets → select an asset.
- In the KUMA web interface, select **Alerts** → click the link with the relevant alert → select the asset in the **Related endpoints** section.
- In the KUMA web interface, select **Events** → search and filter events → select the relevant event → click the link in one of the following fields: SourceAssetID, DestinationAssetID, or DeviceAssetID.

The following information may be displayed in the asset details window:

- **Name**—asset name.

  Assets imported into KUMA retain the names that were assigned to them at the source. You can change these names in the KUMA web interface.

- **Tenant**—the name of the tenant that owns the asset.

- **Asset source**—source of information about the asset. There may be several sources. For instance, information can be added in the KUMA web interface or by using the API, or it can be imported from Kaspersky Security Center, KICS/KATA, and MaxPatrol reports.

  When using multiple sources to add information about the same asset to KUMA, you should take into account the rules for merging asset data.

- **Created**—date and time when the asset was added to KUMA.

- **Updated**—date and time when the asset information was most recently modified.

- **Owner**—owner of the asset, if provided.

- **IP address**—IP address of the asset (if any).

  > If there are several assets with identical IP addresses in KUMA, the asset that was added the latest is returned in all cases when assets are searched by IP address. If assets with identical IP addresses can coexist in your organization's network, plan accordingly and use additional attributes to identify the assets. For example, this may become important during correlation.

- **FQDN**—Fully Qualified Domain Name of the asset, if provided.

- **MAC address**—MAC address of the asset (if any).

- **Operating system**—operating system of the asset.

- **Related alerts**—alerts associated with the asset (if any).

  To view the list of alerts related to an asset, click the **Find in Alerts** link. This opens the **Alerts** tab with the search expression set to filter all assets with the corresponding asset ID.

- **Software info** and **Hardware info**—if the asset software and hardware parameters are provided, they are displayed in this section.

- Asset vulnerability information:

  - **Kaspersky Security Center vulnerabilities**—vulnerabilities of the asset, if provided. This information is available for the assets imported from Kaspersky Security Center.

    If you have configured and enabled integration with Kaspersky Vulnerability Management, vulnerability data is received from this solution. When the Kaspersky Vulnerability Management integration is disabled, data is received from Kaspersky Security Center.

    The header of each vulnerability has the following format: <vulnerability ID> <vulnerable application> <vulnerable version of the application>. The vulnerability information may also contain a brief description of the vulnerability, recommended actions, the CVE IDs of the vulnerability, and a note on whether any malware is known to be exploiting the vulnerability.

You can learn more about the vulnerability by clicking the icon, which opens the Kaspersky Threats portal. You can also update the vulnerabilities list by clicking the **Update** link and requesting updated information from Kaspersky Security Center.

- **KICS/KATA vulnerabilities**—vulnerabilities of the asset, if any. This information is available for the assets imported from KICS/KATA.

- Asset source information:
  - **Last visible**—time when information about the asset was last received from Kaspersky Security Center. This information is available for the assets imported from Kaspersky Security Center.
  - **Host ID**—ID of the Kaspersky Security Center *Network Agent* from which the asset information was received. This information is available for the assets imported from Kaspersky Security Center. This ID is used to determine the uniqueness of the asset in Kaspersky Security Center.
  - **KICS/KATA server IP address** and **KICS/KATA connector ID**—data on the KICS/KATA instance from which the asset was imported.
- **Custom fields**—data written to the asset custom fields.
- Additional information about the protection settings of an asset with Kaspersky Endpoint Security for Windows or Kaspersky Endpoint Security for Linux installed:
  - **KSC extended status ID** – asset status. It can have the following values:
    - OK
    - Critical
    - Warning
  - **KSC extended status** – information about the asset status. For example, **Anti-virus databases were updated too long ago**.
  - **Real-time protection status** – status of Kaspersky applications installed on the asset. For example: **Running (if anti-virus application does not support categories of state Running)**.
  - **Encryption status** – information about asset encryption. For example: **Host doesn't have any encryption rules**.
  - **Spam protection status** – status of anti-spam protection. For example, **Starting**.
  - **Anti-virus protection status of mail servers** – status of the virus protection of mail servers. For example, **Starting**.
  - **Data Leakage Prevention status** – status of data leak protection. For example, **Starting**.
  - **Endpoint Sensor status** – status of data leak protection. For example, **Starting**.
  - **Anti-virus databases last updated** – the version of the downloaded anti-virus databases.
  - **Protection last updated** – the time when the anti-virus databases were last updated.
  - **System last started** – the time when the system was last started.

This information is displayed if the asset was imported from Kaspersky Security Center.

- **Categories**—categories associated with the asset (if any).
- **CII category**—information about whether an asset is a critical information infrastructure (CII) object.

By clicking the **Move to KSC group** button, you can move the asset that you are viewing between Kaspersky Security Center administration groups. You can also click the **Start task** drop-down list to run tasks available on the asset:

- By clicking the **KSC response** button, you can start a Kaspersky Security Center task on the asset.
- By clicking the **KEDR response** button, you can run a Kaspersky Endpoint Detection and Response task on the asset.
- By clicking the **Refresh KSC asset** button, you can run a task to refresh information about the asset from Kaspersky Security Center.

> The tasks are available when integrated with Kaspersky Security Center and when integrated with Kaspersky Endpoint Detection and Response.

Adding assets

You can add asset information to KUMA in the following ways:

- Manually.

  You can add an asset using the KUMA web interface or the API. In this case, you must manually specify the following information: address, FQDN, name and version of the operating system, hardware information. Information about the vulnerabilities of assets cannot be added through the web interface. You can provide information about vulnerabilities if you add assets using the API.

- Import assets.

  You can import assets from Kaspersky Security Center, KICS/KATA, and MaxPatrol reports.

When adding assets, assets that already exist in KUMA can be merged with the assets being added.

Asset merging algorithm:

1. Checking the uniqueness of assets in Kaspersky Security Center or KICS/KATA assets.

   - The uniqueness of an asset imported from Kaspersky Security Center is determined by the **Host ID** parameter, which contains the Kaspersky Security Center Network Agent *Network Agent* identifier. If two assets' IDs differ, they are considered to be separate assets and are not merged.
   - The uniqueness of an asset imported from KICS/KATA is determined by the combination of the **IP address**, **KICS/KATA server IP address**, and **KICS/KATA connector ID** parameters. If any of the parameters of two assets differ they are considered to be separate assets and are not merged.

   If the compared assets match, the algorithm is performed further.

2. Make sure that the values in the **IP**, **MAC**, **FQDN** fields match.

   If at least two of the specified fields match, the assets are combined, provided that the other fields are blank.

Possible matches:

- The FQDN and IP address of the assets match. The **MAC** field is blank.

  The check is performed against the entire array of IP address values. If the IP address of an asset is included in the FQDN, the values are considered to match.

- The FQDN and MAC address of the assets match. The **IP** field is blank.

  The check is performed against the entire array of MAC address values. If at least one value of the array fully matches the FQDN, the values are considered to match.

- The IP address and MAC address of the assets match. The **FQDN** field is blank.

  The check is performed against the entire array of IP- and MAC address values. If at least one value in the arrays is fully matched, the values are considered to match.

3. Make sure that the values of at least one of the **IP**, **MAC**, **FQDN** fields match, provided that the other two fields are not filled in for one or both assets.

   Assets are merged if the values in the field match. For example, if the FQDN and IP address are specified for a KUMA asset, but only the IP address with the same value is specified for an imported asset, the fields match. In this case, the assets are merged.

   For each field, verification is performed separately and ends on the first match.

Examples of asset field comparison are displayed here.

Information about assets can be generated from various sources. If the added asset and the KUMA asset contain data received from the same source, this data is overwritten. For example, a Kaspersky Security Center asset receives a fully qualified domain name, software information, and host ID when imported into KUMA. When importing an asset from Kaspersky Security Center with an equivalent fully qualified domain name, all this data will be overwritten (if it has been defined for the added asset). All fields in which the data can be refreshed are listed in the Updatable data table.

Updatable data

Field name	Update procedure
Name	Selected according to the following priority: • Manually defined. • Received from Kaspersky Security Center. • Received by KICS/KATA.
Owner	The first value from the sources is selected according to the following priority: • Received from Kaspersky Security Center. • Manually defined.
IP address	The data is merged. If the array of addresses contains identical addresses, the copy of the duplicate address is deleted.
FQDN	The first value from the sources is selected according to the following priority: • Received from Kaspersky Security Center. • Received by KICS/KATA. • Manually defined.
MAC address	The data is merged. If the array of addresses contains identical addresses, one of the duplicate addresses is deleted.
Operating system	The first value from the sources is selected according to the following priority: • Received from Kaspersky Security Center. • Received by KICS/KATA. • Manually defined.

Field name	Update procedure
Vulnerabilities	KUMA asset data is supplemented with information from the added assets. In the asset details, data is grouped by the name of the source. Vulnerabilities are eliminated for each source separately.
Software info	Data from KICS/KATA is always recorded (if available). For other sources, the first value is selected according to the following priority: • Received from Kaspersky Security Center. • Manually defined.
Hardware info	The first value from the sources is selected according to the following priority: • Received from Kaspersky Security Center. • Defined via the API.

The updated data is displayed in the asset details. You can view asset details in the KUMA web interface.

This data may be overwritten when new assets are added. If the data used to generate asset information is not updated from sources for more than 30 days, the asset is deleted. The next time you add an asset from the same sources, a new asset is created.

If the KUMA web interface is used to edit asset information that was received from Kaspersky Security Center or KICS/KATA, you can edit the following asset information:

- Name.
- Category.

If asset information was added manually, you can edit the following asset data when editing these assets in the KUMA web interface:

- Name.
- Name of the tenant that owns the asset.
- IP address.
- Fully qualified domain name.
- MAC address.
- Owner.
- Category.
- Operating system.
- Hardware info.

Asset data cannot be edited via the REST API. When importing from the REST API, the data is updated according to the rules for merging asset details provided above.

Adding asset information in the KUMA web interface

To add an asset in the KUMA web interface:

1. In the **Assets** section of the KUMA web interface, click the **Add asset** button.

   The **Add asset** details area opens in the right part of the window.

2. Enter the asset parameters:

   - **Asset name** (required)
   - **Tenant** (required)
   - **IP address** and/or **FQDN** (required) You can specify multiple FQDNs separated by commas.
   - **MAC address**
   - **Owner**

3. If required, assign one or multiple categories to the asset:

   a. Click the tree ( ) button.

   Select categories window opens.

   b. Select the check boxes next to the categories that should be assigned to the asset. You can use the plus ( ) and minus ( ) icons to expand or collapse the lists of categories.

   c. Click **Save**.

   The selected categories appear in the **Categories** fields.

4. If required, add information about the operating system installed on the asset in the **Software** section.

5. If required, add information about asset hardware in the **Hardware info** section.

6. Click **Add**.

   The asset is created and displayed in the assets table in the category assigned to it or in the **Uncategorized assets** category.

Importing asset information and asset vulnerability information from Kaspersky Security Center

All assets that are protected by Kaspersky Security Center are registered in it. You can import into KUMA the information about assets or vulnerabilities of assets that Kaspersky Security Center protects. To do so, you need to configure integration between the applications in advance.

In Kaspersky Security Center integration settings, you can configure the frequency of automatic import of information about assets, and, if necessary, import assets manually. Importing assets manually does not affect the time of the next scheduled import. From the Kaspersky Security Center database, KUMA imports information about devices with installed Kaspersky Security Center Network Agent that has connected to Kaspersky Security Center, that is, has a non-empty 'Connection time' field in the SQL database.

KUMA imports the following device information received from Kaspersky Security Center Network Agents:

- Basic information about the asset: name, address, time of connection to Kaspersky Security Center, hardware information, protection status, anti-virus database versions
- Information about asset attributes: vulnerabilities; software, including the operating system; owners of the asset

By default, basic asset information is imported every hour, and information about asset attributes is imported every 12 hours. Attribute information is imported only for existing assets, not for new or deleted assets.

If a large number of assets are registered in Kaspersky Security Center (tens of thousands hosts), the import task may take a significant amount of time to complete (up to 15–20 hours). The following errors may be encountered during the import process:

```
Kaspersky Security Center assets not fetched. Post "https://<KSC
address>:13299/api/v1.0/login": read tcp <KUMA address>:57498-><KSC address>:13299:
read: connection reset by peer
```

```
Kaspersky Security Center assets not fetched. list child: Resource is unavailable
```

```
Kaspersky Security Center assets not fetched. Post "https://<KSC
address>:13299/api/v1.0/login": EOF
```

To help the import complete sooner and avoid such errors, you need to additionally manage integration settings.

Additional configuration of the integration

For KUMA 3.2 and later, you can specify the number of hosts to be processed per query when importing vulnerability information.

To set the number of hosts:

1. Create a vuln_iterator_config.json file with the following contents:

   ```
   {
   "ksc1.domain.ru": k,
   "ksc2.domain.ru": k
   }
   ```

   where:

   - `ksc1.domain.ru`, `ksc2.domain.ru` are addresses of Kaspersky Security Center servers specified in the KUMA integration settings.
   - `k` sets the number of hosts per query for which information about vulnerabilities is requested. The maximum number of vulnerabilities per query is 10,000.

2. Place the created file:

   - For a single-server KUMA installation, in /opt/kaspersky/kuma
   - For a distributed KUMA installation on multiple servers, run the following command on any cluster controller:

     ```
     export POD=$(k0s kubectl get pods --namespace kuma -l "app=core" -o jsonpath="
     {.items[0].metadata.name}");
     k0s kubectl cp --no-preserve -c core ./vuln_iterator_config.json
     kuma/$POD:/opt/kaspersky/kuma/vuln_iterator_config.json
     ```

   Changes take effect the next time the import task is run.

During the next import of information from Kaspersky Security Center, if KUMA does not receive data about a previously added asset, such an asset is marked as archived. If no information about this asset is received within the next 30 days, the asset is deleted.

> KUMA does not import Kaspersky Security Center assets with the **Last visible** parameter greater than 30 days.

If Kaspersky Security Center encounters errors while running the import tasks, KUMA displays such errors. If basic asset information is not available in KUMA during the import of asset attribute information (for example, if the assets were deleted during the import), the task completes without errors, but the attribute information for these assets is not loaded.

KUMA provides the following ways of importing information about assets or asset vulnerabilities from KSC:

- **Importing asset information and asset vulnerability information for assets of all KSC Servers.**

  To import information about assets or asset vulnerabilities of all Kaspersky Security Center Servers:

  1. In the KUMA web interface, go to the **Assets** section.
  2. Import asset information and asset vulnerability information for assets in one of the following ways:
     - If you want to import information about the basic parameters of assets (protection status, versions of anti-virus databases, hardware), click the **Import KSC assets** button.
     - If you want to import information about other parameters of assets (vulnerabilities, software, owners), click the **Import KSC assets attributes**.
  3. In the displayed window, select the tenant for which you want to perform the import. By default, **All tenants** is selected, which means the import is performed for all tenants.
  4. Click **OK**.

     Information about the assets or asset vulnerabilities of Kaspersky Security Center servers is imported into KUMA.

- **Importing asset information and asset vulnerability information for assets of an individual KSC Server.**

  To import information about assets or asset vulnerabilities of an individual Kaspersky Security Center Server:

  1. In the KUMA web interface, go to the **Settings** → **Kaspersky Security Center** section.

     The **Kaspersky Security Center integration by tenant** window opens.

2. Select the tenant for which you want to perform the import.

   The **Kaspersky Security Center integration** window opens.

3. In the **Connections** table, click the connection to the selected Kaspersky Security Center Server.

   This opens the connection settings window.

4. If the Kaspersky Security Center Server has secondary servers or groups, and you do not want to import information about their assets or vulnerabilities:

   a. Click the **Load hierarchy** button.

   b. Clear the check boxes next to the secondary Servers or groups for which you do not want to perform the import. By default, the check boxes are selected.

   c. If you want to import asset information or asset vulnerability information from new groups, select the **Import assets from new groups** check box. This check box is cleared by default.

   d. Click the **Save** button.

5. Import asset information and asset vulnerability information for assets in one of the following ways:

   - If you want to import information about the basic parameters of assets (protection status, versions of anti-virus databases, hardware), click the **Import KSC assets** button.

   - If you want to import information about other parameters of assets (vulnerabilities, software, owners), click the **Import KSC assets attributes**.

   Information about the assets or asset vulnerabilities of the selected Kaspersky Security Center Server is imported into KUMA.

Importing asset information from MaxPatrol

You can import asset information from the MaxPatrol system into KUMA.

You can use the following import arrangements:

- Importing from reports about scan results of network devices of the MaxPatrol 8 system.

  The import is performed via API using the maxpatrol-tool on the server where the KUMA Core is installed. The tool is included in the KUMA distribution kit and is located in the installer archive in the /kuma-ansible-installer/roles/kuma/files directory.

- Importing data from MaxPatrol VM.

  Data is imported via the API using the kuma_pvtm utility. The tool is included in the KUMA distribution kit and is located in the installer archive in the /kuma-ansible-installer/roles/kuma/files directory.

Imported assets are displayed in the KUMA web interface in the **Assets** section. If necessary, you can edit the settings of assets.

Importing data from MaxPatrol reports

Importing asset information form a report is supported for MaxPatrol 8.

To import asset information from a MaxPatrol report:

1. In MaxPatrol, generate a network asset scan report in **XML file** format and copy the report file to the KUMA Core server. For more details about scan tasks and output file formats, refer to the MaxPatrol documentation.

   > Data cannot be imported from reports in **SIEM integration file** format. The **XML file** format must be selected.

2. Create a file with the token for accessing the KUMA REST API. For convenience, it is recommended to place it into the MaxPatrol report folder. The file must not contain anything except the token.

   Requirements imposed on accounts for which the API token is generated:

   - General administrator, Tenant administrator, Tier 2 analyst, or Tier 1 analyst role.
   - Access to the tenant into which the assets will be imported.
   - Permissions for using API requests GET /api/v3/users/whoami and POST /api/v3/assets/import have been configured.

     > To import assets from MaxPatrol, it is recommended to create a separate user with the minimum necessary set of rights to use API requests.

3. Copy the maxpatrol-tool to the server hosting the KUMA Core and make the tool's file executable by running the following command:

   ```
   chmod +x <path to the maxpatrol-tool file on the server hosting the KUMA Core>
   ```

4. Run the maxpatrol-tool:

   ```
   ./maxpatrol-tool --kuma-rest <KUMA REST API server address and port> --token <path and name of API token file> --tenant <name of tenant where assets will reside> <path and name of MaxPatrol report file> --cert <path to the KUMA Core certificate file>
   ```

   You can download the Core certificate in the KUMA web interface.

   Example: `./maxpatrol-tool --kuma-rest kuma.example.com:7223 --token token.txt --tenant Main example.xml --cert /tmp/ca.cert`

   You can use additional flags and commands for import operations. For example, the command `--verbose, -v` will display a full report on the received assets. A detailed description of the available flags and commands is provided in the table titled Flags and commands of maxpatrol-tool. You can also use the `--help` command to view information on the available flags and commands.

The asset information will be imported from the MaxPatrol report to KUMA. The console displays information on the number of new and updated assets.

```
Example:
inserted 2 assets;
updated 1 asset;
errors occurred: []
```

The utility works as follows when importing assets:

- KUMA overwrites the data of assets imported through the API, and deletes information about their resolved vulnerabilities.
- KUMA skips assets with invalid data. Error information is displayed when using the `--verbose` flag.
- If there are assets with identical IP addresses and fully qualified domain names (FQDN) in the same MaxPatrol report, these assets are merged. The information about their vulnerabilities and software is also merged into one asset.

  When uploading assets from MaxPatrol, assets that have equivalent IP addresses and fully qualified domain names (FQDN) that were previously imported from Kaspersky Security Center are overwritten.

  To avoid this problem, you must configure range-based asset filtering by running the following command:

  `--ignore <IP address ranges>` or `-i <IP address ranges>`

  Assets that satisfy the filtering criteria are not uploaded. For a description of this command, please refer to the table titled *Flags and commands of maxpatrol-tool*.

Flags and commands of maxpatrol-tool

Flags and commands	Description
`--kuma-rest <KUMA REST API server port and address>, -a <KUMA REST API server port and address>`	Address (with the port) of KUMA Core server where assets will be imported. For example, `kuma.example.com:7223`. Port 7223 is used for API requests by default. You can change the port if necessary.
`--token <path and name of API token file>, -t <path and name of API token file>`	Path and name of the file containing the token used to access the REST API. This file must contain only the token. The account for which you are generating an API token must have the General administrator, Tenant administrator, Tier 2 administrator, or Tier 1 administrator role.
`--tenant <tenant name>, -T <tenant name>`	Name of the KUMA tenant into which you want to import assets from the MaxPatrol report.
`--dns <IP address ranges> or -d <IP address ranges>`	This command uses DNS to enrich IP addresses with FQDNs from the specified ranges if the FQDNs for these addresses were not already specified. Example: `--dns 0.0.0.0-9.255.255.255,11.0.0.0-255.255.255,10.0.0.2`
`--dns-server <DNS server IP address>, -s <DNS server IP address>`	Address of the DNS server that the tool must contact to receive FQDN information. Example: `--dns-server 8.8.8.8`
`--ignore <IP address ranges> or -i <IP address ranges>`	Address ranges of assets that should be skipped during import. Example: `--ignore 8.8.0.0-8.8.255.255, 10.10.0.1`
`--verbose, -v`	Output of the complete report on received assets and any errors that occurred during the import process.

`--help, -h`
`help`
	Get reference information on the tool or a command.
	Examples:
	`./maxpatrol-tool help`
	`./maxpatrol-tool <command> --help`

`version`	Get information about the version of the maxpatrol-tool.
`completion`	Creation of an autocompletion script for the specified shell.
`--cert <path to file with the KUMA Core certificate>`	Path to the KUMA Core certificate.

Examples:

- `./maxpatrol-tool --kuma-rest kuma.example.com:7223 --token token.txt --tenant Main example.xml --cert /example-directory/ca.cert` – import assets to KUMA from MaxPatrol report example.xml.
- `./maxpatrol-tool help`—get reference information on the tool.

Possible errors

Error message	Description
must provide path to xml file to import assets	The path to the MaxPatrol report file was not specified.
incorrect IP address format	Invalid IP address format. This error may arise when incorrect IP ranges are indicated.
no tenants match specified name	No suitable tenants were found for the specified tenant name using the REST API.
unexpected number of tenants (%v) match specified name. Tenants are: %v	KUMA returned more than one tenant for the specified tenant name.
could not parse file due to error: %w	Error reading the XML file containing the MaxPatrol report.
error decoding token: %w	Error reading the API token file.
error when importing files to KUMA: %w	Error transferring asset information to KUMA.
skipped asset with no FQDN and IP address	One of the assets in the report did not have an FQDN or IP address. Information about this asset was not sent to KUMA.
skipped asset with invalid FQDN: %v	One of the assets in the report had an incorrect FQDN. Information about this asset was not sent to KUMA.
skipped asset with invalid IP address: %v	One of the assets in the report had an incorrect IP address. Information about this asset was not sent to KUMA.
KUMA response: %v	An error occurred with the specified report when importing asset information.
unexpected status code %v	An unexpected HTTP code was received when importing asset information from KUMA.

Importing asset information from MaxPatrol VM

The KUMA distribution kit includes the kuma-ptvm utility, which consists of an executable file and a configuration file. The utility is supported on Windows and Linux operating systems. The utility allows you to connect to the MaxPatrol VM API to get data about devices and their attributes, including vulnerabilities, and also lets you edit asset data and import data using the KUMA API. Data import is supported for MaxPatrol VM versions from 1.1 to 2.7 inclusive.

Configuring the import of asset information from MaxPatrol VM to KUMA involves the following steps:

1. Preparing KUMA and MaxPatrol VM.

   You must create user accounts and a KUMA token for API operations.

2. Creating a configuration file with data export and import settings.

   Depending on the required data set, use one of the following configuration files:

   - `kuma-ptvm-config.yaml` for importing information about assets and vulnerabilities.
   - `kuma-ptvm-vulnerable-assets-config.yaml` for importing information about assets and vulnerabilities with optional filtering.

Both files contain required and optional settings. Fill in the required settings and, if necessary, specify additional data filtering conditions. As a result, only assets that match the specified conditions are imported into KUMA.

The `kuma-ptvm-vulnerable-assets-config.yaml` file additionally contains the `Vulnerabilities assets settings` section, in which you can manage vulnerability information import settings.

3. Exporting data from MaxPatrol VM and importing it into KUMA using the kuma-ptvm utility.

   Run the utility with the appropriate configuration file:

   - To import asset information:

     ```
     ./kuma-ptvm --config <path to kuma-ptvm-config.yaml> --download --upload
     ```

   - To import information about assets and vulnerabilities with optional filtering:

     ```
     ./kuma-ptvm vulnerable-assets-api --config <path to kuma-ptvm-vulnerable-assets-config.yaml> --download --
     upload
     ```

   When you run this command, the data is first exported from MaxPatrol VM and saved in the directory of the utility. Information for each tenant is saved to a separate file in JSON format.

   If necessary, you can edit the received files. After that, the data from the files is imported into KUMA.

When re-importing existing assets, assets that already exist in KUMA are overwritten. In this way, fixed vulnerabilities are removed.

Known limitations

If the same IP address is specified for two assets with different FQDNs, KUMA imports such assets as two different assets; the assets are not combined.

If an asset has two softwares with the same data in the name, version, vendor fields, KUMA imports this data as one software, despite the different software installation paths in the asset.

If in the `kuma-ptvm-config.yaml` configuration file, you set strict_import to false, data from MaxPatrol is imported for all assets, including those without fields that KUMA requires and those with field values that KUMA does not allow. If the FQDN of an asset contains a space or underscore ("_"), data for such assets is not imported into KUMA, and the log indicates that the assets were skipped during import.

If an error occurs during import, error details are logged and the import stops.

Preparatory actions

1. Create a separate user account in KUMA and in MaxPatrol VM with the minimum necessary set of permissions to use API requests.

2. Create user accounts for which you will lager generate an API token.

Requirements imposed on accounts for which the API token is generated:

- General administrator, Tenant administrator, Tier 2 analyst, or Tier 1 analyst role.
- Access to the tenant into which the assets will be imported.
- In the user account, under **API access rights**, the check box is selected for POST/api/v3/assets/import.

3. Generate a token for access to the KUMA REST API.

Creating the configuration file

To create the configuration file:

1. Go to the KUMA installer folder by executing the following command:

```
cd kuma-ansible-installer/roles/kuma/files/
```

2. Extract the kuma-ptvm.tar.gz archive by running the following command:
`tar -xvf kuma-ptvm.tar.gz`

3. Copy the template and create a configuration file depending on how you want to import assets.

   - For standard import of asset data:

```
cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
```

   - If you need to additionally manage the vulnerability data import settings:

```
cp kuma-ptvm-vulnerable-assets-config-template.yaml kuma-ptvm-vulnerable-assets-config.yaml
```

4. Depending on the chosen method of importing assets, edit the settings in the kuma-ptvm-config.yaml configuration file or the settings in the kuma-ptvm-vulnerable-assets-config-template.yaml configuration file.

5. Save the changes to the file.

The configuration file will be created. Go to the Importing asset data step.

Importing asset data

To import asset information from MaxPatrol VM into KUMA, use the kuma-ptvm utility with the configuration file created at the previous step.

To import asset information:

1. If you want to import asset information from MaxPatrol VM into KUMA without intermediate verification of the exported data, run the download an upload commands at the same time. Select the command depending on the configuration file you are using:

   - For `kuma-ptvm-config.yaml`:

     ```
     ./kuma-ptvm --config <path> --download --upload
     ```

   - For `kuma-ptvm-vulnerable-assets-config.yaml`:

     ```
     kuma-ptvm vulnerable-assets-api --config <path> --download --upload
     ```

   where:

   <path> is the full path to the corresponding configuration file: `kuma-ptvm-config.yaml` or `kuma-ptvm-vulnerable-assets-config.yaml`.

2. If you want to check the correctness of data exported from MaxPatrol VM before importing it into KUMA, first perform just the export:

   - For `kuma-ptvm-config.yaml`:

     ```
     ./kuma-ptvm --config <path> --download
     ```

   - For `kuma-ptvm-vulnerable-assets-config.yaml`:

     ```
     ./kuma-ptvm vulnerable-assets-api --config <path> --download
     ```

   where:

   <path> is the full path to the corresponding configuration file: `kuma-ptvm-config.yaml` or `kuma-ptvm-vulnerable-assets-config.yaml`.

   If necessary, you can use the `--cvss-version <CVSS version number>` option to specify the version of CVSS for which you want to load asset vulnerability values. Available values:

   - `2` loads only CVSS version 2 values.
   - `3` loads only CVSS version 3 values. If a vulnerability is described only for version 2, the CVSS field is empty.
   - `latest` (default) loads the values of the latest available version of CVSS. If the vulnerability does not have a CVSS version 3 value, the version 2 value is used.

   Examples:

   ```
   ./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 2 --download
   ./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 3 --download
   ./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version latest --download
   ```

   where:

<path> is the full path to the corresponding configuration file: `kuma-ptvm-config.yaml` or `kuma-ptvm-vulnerable-assets-config.yaml`.

The utility creates a separate JSON file for each tenant specified in the configuration file. A tenants file is also created, containing a list of files from which data will be imported into KUMA. All files are saved in the utility's directory.

If necessary, review and edit the exported data:

- Assign assets to their corresponding tenants.
- Manually transfer asset data from the 'default' tenant file to the files of the relevant tenants.
- In the 'tenants' file, edit the list of tenants whose assets you want to import into KUMA.

a. After reviewing the asset information, import it into KUMA:

- For `kuma-ptvm-config.yaml`:

```
./kuma-ptvm --config <path> --upload
```

- For `kuma-ptvm-vulnerable-assets-config.yaml`:

```
./kuma-ptvm vulnerable-assets-api --config <path> --upload
```

where:

<path> is the full path to the corresponding configuration file: `kuma-ptvm-config.yaml` or `kuma-ptvm-vulnerable-assets-config.yaml`.

To view information about the available commands of the utility, run the `--help` command.

The asset information is imported from MaxPatrol VM to KUMA. The console displays information on the number of new and updated assets.

Possible errors

When running the kuma-ptvm utility, the `tls: failed to verify certificate: x509: certificate is valid for localhost` error may be returned.

Solution.

- Issue a certificate in accordance with the MaxPatrol documentation. We recommend resolving the error in this way.
- Disable certificate validation.

  To disable certificate validation, add the following line to the configuration file in the `MaxPatrol settings` section:

  `ignore_server_cert: true`

As a result, the utility is started without errors.

Settings of the kuma-ptvm-config.yaml configuration file

The table lists the settings that you can specify in the `kuma-ptvm-config.yaml` file.

Description of settings in the kuma-ptvm-config.yaml configuration file

Setting	Description	Values
`General settings` section		
`log_level`	Optional setting. Logging level.	Available values: • `trace` • `info` • `warning` • `error` Default setting: `info`.
`period`	Optional setting. Data for assets that have changed during the specified period is exported from MaxPatrol.	No limitations apply. Default setting: `30d`.
`strict_import`	Optional setting. When exporting assets from MaxPatrol, check if the required fields for KUMA are filled. Do not export unverified assets from MaxPatrol.	Available values: • `true` to check for the presence of fields that are required for KUMA. • `false` to skip the check for the presence of fields that are required for KUMA. The default value is `false`. We recommend specifying `true` when exporting assets from MaxPatrol, this lets you detect and fix possible errors in JSON files before you import assets into KUMA.
`parallel_downloading`	Optional setting. Sets the downloading mode when importing data from MaxPatrol.	Available values: • `true` downloads CSV files in parallel. • `false` downloads CSV files sequentially to reduce the load on MaxPatrol. The default setting is `true`. We recommend specifying `false` if you need to reduce the load on MaxPatrol during data import.
`KUMA settings` section		
`endpoint`	Required setting. URL of the KUMA API server. For example, kuma.example.com:7223	–
`token`	Required setting. KUMA API token.	–
`ignore_server_cert`	Optional setting. Validation of the KUMA certificate.	Available values: • `true` to disable KUMA certificate validation. • `false` to enable KUMA certificate validation. This setting is not included in the configuration file template. You can manually add this setting with a `true` value, which will prevent the kuma-ptvm utility from validating the certificate at startup.
`MaxPatrol settings` section		
`endpoint`	Required setting. URL of the MaxPatrol API server.	–
`user`	Optional setting. MaxPatrol API user name.	–
`password`	Optional setting. MaxPatrol API user password.	–
`secret`	Optional setting. MaxPatrol API secret.	–

Setting	Description	Values
`token`	Optional setting. MaxPatrol API token.	To gain access to the MaxPatrol server through the API, specify either the values of the `user`, `password`, and `secret` parameters, or the value of the `token` parameter.
`ignore_server_cert`	Optional setting. Validation of the MaxPatrol certificate.	Available values: • `true` to disable the validation of the MaxPatrol certificate. • `true` to enable MaxPatrol certificate validation. This setting is not included in the configuration file template. You can manually add this setting with a `true` value if you get the `tls: failed to verify certificate: x509: certificate is valid for localhost` error. In that case, the kuma-ptvm utility does not validate the certificate when it is started. We recommend issuing a certificate in accordance with the MaxPatrol documentation as the preferred way of resolving the error.
`Vulnerability filter` section		
`only_exploitable`	Optional setting. Export from MaxPatrol only assets with vulnerabilities for which exploits are known.	Available values: • `true` to export only assets with vulnerabilities for which exploits are known. • `false` to export all assets. Default setting: `false`.
`min_severity`	Optional setting. Import only vulnerabilities of the specified level or higher.	Available values: • `low` • `medium` • `high` • `critical` Default value: `low`.
`Tenant map` section		
`id`	Required setting. Tenant ID in KUMA. Assets are assigned to tenants in the order in which tenants are specified in the configuration file: the higher a tenant is in the list, the higher its priority. This means you can specify overlapping subnets.	–
`fqdn`	Optional setting. Regular expression for searching the FQDN of an asset.	–
`networks`	Optional setting. One or more subnets.	–
`default_tenant`	Optional setting. The default KUMA tenant for data about assets that could not be allocated to tenants specified in the 'Tenants' section.	–

Settings in the kuma-ptvm-vulnerable-assets-config-template.yaml configuration file

The table lists the settings that you can specify in the `kuma-ptvm-vulnerable-assets-config-template.yaml` file.

Description of the settings in the kuma-ptvm-vulnerable-assets-config-template.yaml configuration file

Setting	Description	Values
`General settings` section		
`log_level`	Optional setting. Logging level.	Available values: • `trace` • `info` • `warning` • `error` Default setting: `info`.
`strict_import`	Optional setting. When exporting assets from MaxPatrol, check if the required fields for KUMA are filled. Do not export unverified assets from MaxPatrol.	Available values: • `true` to check for the presence of fields that are required for KUMA. • `false` to skip the check for the presence of fields that are required for KUMA. The default value is `false`. We recommend specifying `true` when exporting assets from MaxPatrol, this lets you detect and fix possible errors in JSON files before you import assets into KUMA.
`KUMA settings` section		
`endpoint`	Required setting. URL of the KUMA API server. For example, kuma.example.com:7223	–
`token`	Required setting. KUMA API token.	–
`MaxPatrol settings` section		
`endpoint`	Required setting. URL of the MaxPatrol API server.	–
`token`	Optional setting. MaxPatrol API token.	For API access to the MaxPatrol server, you need to specify the `token` setting.
`Vulnerable Assets API Parameters` section A limitation applies: the `from` and `to` parameters are available in the current Swagger contract, but their support depends on the version of PTVM you have deployed.		
`groups`	Optional setting. List of asset group IDs that are used for filtering. Only assets belonging to the specified groups are included in the import.	Example: 4b7d711f-ae35-4c94-8625-4cfabf5fb99e
`statuses`	Optional setting. Vulnerability status for assets to be filtered.	Available values: • `new` means the vulnerability is new. • `inProgress` means the vulnerability is being fixed. • `awaitingFix` means the vulnerability is waiting to be fixed. • `excluded` means the vulnerability has been excluded from processing. • `fixed` means the vulnerability has been fixed. • `overdue` means the vulnerability is past its fixing deadline. • `stale` means the vulnerability is obsolete.
`severities`	Optional setting. Severity of asset vulnerabilities for filtering.	Available values: • `none` means a severity is not set. • `low` • `medium` • `high` • `critical`
`from`	Optional setting. The start date and time of the for filtering by the date of the last audit of the asset, inclusive. UTC.	Example: [TBD]

Setting	Description	Values
`to`	Optional setting. The end date and time of the for filtering by the date of the last audit of the asset, inclusive. UTC.	Example: [TBD]
`Vulnerability filter` section		
`only_exploitable`	Optional setting. Export from MaxPatrol only assets with vulnerabilities for which exploits are known.	Available values: • `true` to export only assets with vulnerabilities for which exploits are known. • `false` to export all assets. Default setting: `false`.
`Tenant map` section		
`id`	Required setting. Tenant ID in KUMA. Assets are assigned to tenants in the order in which tenants are specified in the configuration file: the higher a tenant is in the list, the higher its priority. This means you can specify overlapping subnets.	–
`fqdn`	Optional setting. Regular expression for searching the FQDN of an asset.	–
`networks`	Optional setting. One or more subnets.	–
`default_tenant`	Optional setting. The default KUMA tenant for data about assets that could not be allocated to tenants specified in the 'Tenants' section.	–

Importing asset information from KICS for Networks

After configuring KICS for Networks integration, tasks to obtain data about KICS for Networks assets are created automatically. This occurs:

- Immediately after creating a new integration.
- Immediately after changing the settings of an existing integration.
- According to a regular schedule every several hours. Every 12 hours by default. The schedule can be changed.

Account data update tasks can be created manually.

To start a task to update KICS/KATA asset information for a tenant:

1. In the KUMA web interface, open the **Settings** → **KICS/KATA** section.
2. Select the relevant tenant.

   This opens the **KICS/KATA server integration** window.
3. Click the **Import assets** button.

   A task to receive account data from the selected tenant is added to the **Task manager** section of the KUMA web interface.

Examples of asset field comparison during import

Each imported asset is compared to the matching KUMA asset.

Checking for two-field value match in the IP, MAC, and FQDN fields

Compared assets	Compared fields		
	FQDN	IP	MAC
KUMA asset	Filled in	Filled in	Empty
Imported asset 1	Filled in, matching	Filled in, matching	Filled in
Imported asset 2	Filled in, matching	Filled in, matching	Empty
Imported asset 3	Filled in, matching	Empty	Filled in
Imported asset 4	Empty	Filled in, matching	Filled in
Imported asset 5	Filled in, matching	Empty	Empty
Imported asset 6	Empty	Empty	Filled in

Comparison results:

- Imported asset 1 and KUMA asset: the FQDN and IP fields are filled in and match, no conflict in the MAC fields between the two assets. The assets are merged.
- Imported asset 2 and KUMA asset: the FQDN and IP fields are filled in and match. The assets are merged.
- Imported asset 3 and KUMA asset: the FQDN and MAC fields are filled in and match, no conflict in the IP fields between the two assets. The assets are merged.
- Imported asset 4 and KUMA asset: the IP fields are filled in and match, no conflict in the FQDN and MAC fields between the two assets. The assets are merged.
- Imported asset 5 and KUMA asset: the FQDN fields are filled in and match, no conflict in the IP and MAC fields between the two assets. The assets are merged.
- Imported asset 6 and KUMA asset: no matching fields. The assets are not merged.

Checking for single-field value match in the IP, MAC, and FQDN fields

Compared assets	Compared fields		
	FQDN	IP	MAC
KUMA asset	Empty	Filled in	Empty
Imported asset 1	Filled in	Filled in, matching	Filled in
Imported asset 2	Filled in	Filled in, matching	Empty

Compared assets	Compared fields		
	FQDN	IP	MAC
Imported asset 3	Filled in	Empty	Filled in
Imported asset 4	Empty	Empty	Filled in

Comparison results:

- Imported asset 1 and KUMA asset: the IP fields are filled in and match, no conflict in the FQDN and MAC fields between the two assets. The assets are merged.
- Imported asset 2 and KUMA asset: the IP fields are filled in and match, no conflict in the FQDN and MAC fields between the two assets. The assets are merged.
- Imported asset 3 and KUMA asset: no matching fields. The assets are not merged.
- Imported asset 4 and KUMA asset: no matching fields. The assets are not merged.

Working with Kaspersky Security Center tasks

You can connect Kaspersky Security Center assets to KUMA and download database and application module updates to these assets, or run an anti-virus scan on them by using Kaspersky Security Center tasks. Tasks are started in the KUMA web interface.

To run Kaspersky Security Center tasks on assets connected to KUMA, it is recommended to use the following script:

1. **Creating a user account in the Kaspersky Security Center Administration Console**

   The credentials of this account are used when creating a secret to establish a connection with Kaspersky Security Center, and can be used to create a task.

   For more details about creating a user account and assigning permissions to a user, please refer to the *Kaspersky Security Center Help Guide*.

2. Creating KUMA tasks in Kaspersky Security Center

3. Configuring KUMA integration with Kaspersky Security Center

4. Importing asset information from Kaspersky Security Center into KUMA

5. Assigning a category to the imported assets

   After import, the assets are automatically placed in the **Uncategorized devices** group. You can assign one of the existing categories to the imported assets, or create a category and assign it to the assets.

6. **Running tasks on assets**

   You can manually start tasks in the asset information or configure tasks to start automatically.

Creating KUMA tasks in Kaspersky Security Center

You can run the anti-virus database and application module update task, and the virus scan task on Kaspersky Security Center assets connected to KUMA. The assets must have Kaspersky Endpoint Security for Windows or Linux installed. The tasks are created in Kaspersky Security Center Web Console.

For more details about creating the *Update* and *Virus scan* tasks on the assets with Kaspersky Endpoint Security for Windows, refer to the *Kaspersky Endpoint Security for Windows* Help Guide.

For more details about creating the *Update* and *Virus scan* tasks on the assets with Kaspersky Endpoint Security for Linux, refer to the *Kaspersky Endpoint Security for Linux* Help Guide.

Task names must begin with "kuma" (not case-sensitive and without quotations). For example, `KUMA antivirus check`. Otherwise, the task is not displayed in the list of available tasks in the KUMA web interface.

Starting Kaspersky Security Center tasks manually

You can manually run the anti-virus database, application module update task, and the anti-virus scan task on Kaspersky Security Center assets connected to KUMA. The assets must have Kaspersky Endpoint Security for Windows or Linux installed.

First, you need to configure the integration of Kaspersky Security Center with KUMA and create tasks in Kaspersky Security Center.

To manually start a Kaspersky Security Center task:

1. In the **Assets** section of the KUMA web interface, select the asset that was imported from Kaspersky Security Center.

   The **Asset details** window opens.

2. Click the **KSC response** button.

   This button is displayed if the connection to the Kaspersky Security Center that owns the selected asset is enabled.

3. In the opened **Select task** window, select the check boxes next to the tasks that you want to start, and click the **Start** button.

Kaspersky Security Center starts the selected tasks.

Some types of tasks are available only for certain assets.

You can obtain vulnerability and software information only for assets running a Windows operating system.

Starting Kaspersky Security Center tasks automatically

You can configure the automatic start of the anti-virus database and application module update task and the virus scan task for Kaspersky Security Center assets connected to KUMA. The assets must have Kaspersky Endpoint Security for Windows or Linux installed.

First, you need to configure the integration of Kaspersky Security Center with KUMA and create tasks in Kaspersky Security Center.

Configuring automatic start of Kaspersky Security Center tasks includes the following steps:

Step 1. Adding a correlation rule

To add a correlation rule:

1. In the KUMA web interface, select the **Resources** section.

2. Select **Correlation rules** and click the **Add correlation rule** button.

3. On the **General** tab, specify the following settings:

   a. In the **Name** field, define the rule name.

   b. In the **Tenant** drop-down list, select the tenant that owns the resource.

   c. In the **Type** drop-down list, select **simple**.

   d. In the **Propagated fields** field, add the following fields: DestinationAssetID.

e. If required, define the values for the following fields:

- In the **Rate limit** field, define the maximum number of times per second that the rule will be triggered.
- In the **Severity** field, define the severity of alerts and correlation events that will be created as a result of the rule being triggered.
- In the **Description** field, provide any additional information.

4. On the **Selectors** → **Settings** tab:

a. In the **Filter** drop-down list, select **Create new**.

b. In the **Conditions** field, click the **Add group** button.

c. In the operator field for the group you added, select **AND**.

d. Add a condition for filtering by the DeviceProduct field value:

1. In the **Conditions** field, click the **Add condition** button.
2. In the condition field, select **If**.
3. In the **Left operand** field, select event field.
4. In the 'Event field' field, select DeviceProduct.
5. In the Operator field, select =.
6. In the **Right operand** field, select **constant**.
7. In the **value** field, enter KSC.

e. Add a condition for filtering by the Name field value:

1. In the **Conditions** field, click the **Add condition** button.
2. In the condition field, select **If**.
3. In the **Left operand** field, select event field.
4. In the event field, select Name.
5. In the Operator field, select =.
6. In the **Right operand** field, select **constant**.
7. In the **value** field, enter the name of the event. When this event is detected, the task is started automatically.

   For example, if you want the *Anti-Virus scan* task to start when Kaspersky Security Center registers a *Malicious object detected* event, specify this name in the **value** field.

   You can view the event name in the **Name** field of the event details.

5. On the **Actions** tab, specify the following settings:

   a. In the **Actions** section, open the **On every event** drop-down list.

   b. Select the **Output** check box.

      You do not need to fill in other fields.

6. Click the **Save** button.

The correlation rule will be created.

Step 2. Creating a correlator

Start the Correlator Installation Wizard. At step 3 of the wizard, select the correlation rule that you added while following these steps.

> The DeviceHostName field must display the domain name (FQDN) of the asset. If it is not displayed, create a DNS record for this asset and create a DNS enrichment rule at step 4 of the wizard.

Step 3. Adding a filter

To add a filter:

1. In the KUMA web interface, select the **Resources** section.

2. Select **Filters** and click the **Add filter** button.

3. In the **Name** field, specify the filter name.

4. In the **Tenant** drop-down list, select the tenant that owns the resource.

5. In the **Conditions** field, click the **Add group** button.

6. In the operator field for the group you added, select **AND**.

7. Add a condition for filtering by the DeviceProduct field value:

   a. In the **Conditions** field, click the **Add condition** button.

   b. In the condition field, select **If**.

   c. In the **Left operand** field, select event field.

   d. In the 'Event field' field, select Type.

   e. In the Operator field, select =.

   f. In the **Right operand** field, select **constant**.

   g. In the **value** field, enter 3.

8. Add a condition for filtering by the Name field value:

   a. In the **Conditions** field, click the **Add condition** button.

   b. In the condition field, select **If**.

   c. In the **Left operand** field, select event field.

   d. In the event field, select Name.

   e. In the Operator field, select =.

   f. In the **Right operand** field, select **constant**.

   g. In the **value** field, enter the name of the correlation rule created at Step 1.

Step 4. Adding a response rule

To add a response rule:

1. In the KUMA web interface, select the **Resources** section.

2. Select **Response rules** and click the **Add response rule** button.

3. In the **Name** field, define the rule name.

4. In the **Tenant** drop-down list, select the tenant that owns the resource.

5. In the **Type** drop-down list, select **Response via KSC**.

6. In the **Kaspersky Security Center task** drop-down list, select the Kaspersky Security Center task you want to start.

7. In the **Event field** drop-down list, select the DestinationAssetID.

8. In the **Workers** field, specify the number of workers that the service can run simultaneously to process events in parallel. Specify a positive integer number from 0 to 999. If 0 is specified, the number of logical CPU cores is used.

9. In the **Description** field, you can add up to 4,000 Unicode characters.

10. In the **Filter** drop-down list, select the filter added at Step 3 of this instruction.

To send requests to Kaspersky Security Center, you must ensure that Kaspersky Security Center is available over the UDP protocol.

If response rules are owned by the Shared tenant, then the tasks from the Kaspersky Security Center server to which the Main tenant is connected are displayed as Kaspersky Security Center tasks available for selection.

If a response rule has a selected task that is absent from the Kaspersky Security Center server that the tenant is connected to, the task is not performed for assets of this tenant. This situation could arise when two tenants are using a common correlator, for example.

Step 5. Adding a response rule to the correlator

To add a response rule to the correlator:

1. In the KUMA web interface, select the **Resources** section.

2. Select **Correlators**.

3. In the list of correlators, select the correlator added at Step 2 of this instruction.

4. In the steps tree, select **Response rules**.

5. Then click the **Add** button.

6. In the **Response rule** drop-down list, select the rule added at step 4 of these instructions.

7. In the steps tree, select **Setup validation**.

8. Click the **Save and restart services** button.

9. Click the **Save** button.

   The response rule will be added to the correlator.

The automatic start will be configured for the anti-virus database and application module update task and the virus scan task on Kaspersky Security Center assets connected to KUMA. The tasks are started when a threat is detected on the assets and KUMA receives the corresponding events.

Checking the status of Kaspersky Security Center tasks

In the KUMA web interface, you can check whether a Kaspersky Security Center task was started or whether a search for events owned by the collector listening for Kaspersky Security Center events was completed.

To check the status of Kaspersky Security Center tasks:

1. In KUMA, select **Resources** → **Active services**.

2. Select the collector that is configured to receive events from the Kaspersky Security Center server and click the **Go to Events** button.

   A new browser tab will open in the **Events** section of KUMA. The table displays events from the Kaspersky Security Center server. The status of the tasks can be seen in the **Name** column.

Kaspersky Security Center event fields:

- **Name**—status or type of the task.
- **Message**—message about the task or event.
- **FlexString<number>Label**—name of the attribute received from Kaspersky Security Center. For example, `FlexString1Label=TaskName`.
- **FlexString<number>**—value of the FlexString<number>Label attribute. For example, `FlexString1=Download updates`.
- **DeviceCustomNumber<number>Label**—name of the attribute related to the task state. For example, `DeviceCustomNumber1Label=TaskOldState`.
- **DeviceCustomNumber<number>**—value related to the task state. For example, `DeviceCustomNumber1=1` means the task is executing.
- **DeviceCustomString<number>Label**—name of the attribute related to the detected vulnerability: for example, a virus name, affected application.
- **DeviceCustomString<number>**—value related to the detected vulnerability. For example, the attribute-value pairs `DeviceCustomString1Label=VirusName` and `DeviceCustomString1=EICAR-Test-File` mean that the EICAR test virus was detected.

Assigning a category to an asset

To assign a category to one asset:

1. In the KUMA web interface, go to the **Assets** section.

2. Select the category with the relevant assets.

   The assets table is displayed.

3. Select an asset.

4. In the opened window, click the **Edit** button.

5. In the **Categories** field, click the button.

6. Select a category.

> If you want to move an asset to the **Uncategorized assets** section, you must delete the existing categories for the asset by clicking the ✕ button.

7. Click the **Save** button.

The category will be assigned.

To assign a category to multiple assets:

1. In the KUMA web interface, go to the **Assets** section.
2. Select the category with the relevant assets.
   The assets table is displayed.
3. Select the check boxes next to the assets for which you want to change the category.
4. Click the **Link to category** button.
5. In the opened window, select a category.
6. Click the **Save** button.

The category will be assigned.

> Do not assign the `Categorized assets` category to assets.

Linking a group of assets to a category

To link a group of assets to a category:

1. In the **Assets** section of the KUMA web interface, select the check box in the heading of the table of assets.
2. Select all assets visible on the page or all assets that match the selection condition.
   The **Link to category** button becomes active and opens the available categories.
3. Click the **Link to category** button and select one or more categories to link to.
4. Click **OK**.
   Assets are linked to the selected categories or folder.

Unlinking a group of assets from a category

To unlink a group of assets from a category:

1. Select one category (tenant) in the navigation pane.

   The list of assets in that category is displayed.

   The **Clean category** button is added to the folder properties.

2. In the context menu of the category, select **Clean category**.

   A dialog box is displayed with a confirmation prompt and the number of assets that will be unlinked.

   This option lets you unlink all assets in the selected category, not only those that are visible on the page. Assets in child categories are not unlinked.

3. In the dialog box, click **OK**.

   All selected assets are unlinked from the selected category.

Editing the parameters of assets

In KUMA, you can edit asset parameters. All the parameters of manually added assets can be edited. For assets imported from Kaspersky Security Center, you can only change the name of the asset and its category.

To change the parameters of an asset:

1. In the **Assets** section of the KUMA web interface, click the asset that you want to edit.

   The **Asset details** area opens in the right part of the window.

2. Click the **Edit** button.

   The **Edit asset** window opens.

3. Make the changes you need in the available fields:

   - **Asset name** (required) This is the only field available for editing if the asset was imported from Kaspersky Security Center or KICS/KATA.
   - **IP address** and/or **FQDN** (required) You can specify multiple FQDNs separated by commas.
   - **MAC address**
   - **Owner**
   - **Software info**:
     - **OS name**
     - **OS build**
   - **Hardware info**:

     Hardware parameters

You can add information about asset hardware to the **Hardware info** section:

Available fields for describing the asset CPU:

- **CPU name**
- **CPU frequency**
- **CPU core count**

  You can add CPUs to the asset by using the **Add CPU** link.

Available fields for describing the asset disk:

- **Disk free bytes**
- **Disk volume**

  You can add disks to the asset by using the **Add disk** link.

Available fields for describing the asset RAM:

- **RAM frequency**
- **RAM total bytes**

Available fields for describing the asset network card:

- **Network card name**
- **Network card manufacture**
- **Network card driver version**

  You can add network cards to the asset by using the **Add network card** link.

- Custom fields.
- CII category.

4. Assign or change the category of the asset:

   a. Click the tree ( ) button.
   Select categories window opens.

   b. Select the check boxes next to the categories that should be assigned to the asset.

   c. Click **Save**.

The selected categories appear in the **Categories** fields.

> You can also select the asset and then drag and drop it into the relevant category. This category will be added to the list of asset categories.

Do not assign the `Categorized assets` category to assets.

5. Click the **Save** button.

   Asset parameters have been changed.

Archiving assets

In KUMA, the archival functionality is available for the following types of assets:

- For assets imported from Kaspersky Security Center and KICS.

  If KUMA cannot not receive information about the asset after ten import attempts, the asset is automatically archived and is stored in the database for the time that you can specify in the **TTL for archived assets (days)** setting. The default setting is 0 days. This means that archived assets are stored indefinitely. An archived asset becomes active if KUMA receives information about the asset from the source before the retention period for archived assets expires.

- Combined assets

  When importing, KUMA performs a check for uniqueness among assets imported from Kaspersky Security Center and KICS, and among manually added assets. If the fields of an imported asset and a manually added asset match, the assets are combined into a single asset, which is considered imported and can become archived.

Assets added manually in the console or using the API are not archived.

An asset becomes archived under the following conditions:

- KUMA did not receive information about the asset from Kaspersky Security Center or KICS/KATA after ten import attempts.

- Disabled integration with Kaspersky Security Center.

  If you disable integration with Kaspersky Security Center, the asset is considered active for 30 days. After 30 days, the asset is automatically **TTL for archived assets (days)**.

An asset is not updated in the following cases:

- Information about the Kaspersky Security Center asset has not been updated for more than the retention period of archived assets.

- Information about the asset does not exist in Kaspersky Security Center or KICS/KATA.

- Connection with the Kaspersky Security Center server has not been established for more than 30 days.

Archived assets that participate in dynamic categorization remain archived. An archived asset can have its CII category assigned or changed. If such an asset ends up in an alert or incident, the CII category of the alert or incident also changes, which may affect the visibility of the alert or incident for users with restricted CII access.

To configure the archived assets retention period:

1. In the KUMA web interface, select the **Settings** → **Assets** section.

   This opens the **Assets** window.

2. Enter the new value in the **TTL for archived assets (days)** field.

   The default setting is 0 days. This means that archived assets are stored indefinitely.

3. Click **Save**.

The retention period for archived assets is configured.

Information about the archived asset remains available for viewing in the alert and incident card.

To view an archived asset card:

1. In the KUMA web interface, select the **Alerts** or **Incidents** section.

   A list of alerts or incidents is displayed.

2. Open the alert or incident card linked to the archived asset.

   You can view the information in the archived asset card.

Deleting assets

If you no longer need to receive information from an asset or information about the asset has not been updated for a long time, you can have KUMA delete the asset. Deletion can be performed by the General administrator, Tenant administrator, Tier 2 analysts, and Tier 1 analysts. If an asset was deleted, but KUMA once again begins receiving information about that asset from Kaspersky Security Center, KUMA recreates the asset with a new ID.

In KUMA, you can delete assets in the following ways:

- Automatically.

  KUMA automatically deletes only archived assets. KUMA deletes an archived asset if the information about the asset has not been updated for longer than the retention period of archived assets.

- Manually.

To delete an asset manually:

1. In KUMA web interface, in the **Assets** section, click the asset that you want to delete.

   This opens the **Asset information** window in the right-hand part of the web interface.

2. Click the **Delete** button.

   A confirmation window opens.

3. Click **OK**.

The asset is deleted and no longer appears in the alert or incident card.

Bulk deletion of assets

In the KUMA web interface, you can select multiple assets using a filter and delete all selected assets.

To delete assets, you must have rights to delete assets.

Bulk deletion of assets

To delete all selected assets:

1. In the **Assets** section of the KUMA web interface, select the category that contains the relevant assets.

   A table of assets is displayed.

2. Select the check box in the heading of the table of assets.

   You can delete all assets or all assets currently displayed on the page.

3. Click **Select all in page** or **Select all**.

   The **Delete** button becomes active.

4. Click the **Delete** button.

   This opens a window prompting you to confirm deletion and telling you that deleted assets will not be available in alerts, incidents, and widgets.

   In the lower part of the page, the number of assets selected for deletion is displayed.

5. Click **OK**.

   If you clicked **Select all**, you must enter the displayed generated string into the text box in the window to confirm deletion.

All selected assets are deleted.

Deleting asset folders

To delete a folder, you can either unlink all assets from the folder (which unlinks the assets but not does not delete them) and then delete the folder itself, or delete all assets and then delete the folder.

Updating third-party applications and fixing vulnerabilities on Kaspersky Security Center assets

You can update third-party applications (including Microsoft applications) that are installed on Kaspersky Security Center assets, and fix vulnerabilities in these applications.

First you need to create the *Install required updates and fix vulnerabilities* task on the selected Kaspersky Security Center Administration Server with the following settings:

- Application—Kaspersky Security Center.
- Task type—*Install required updates and fix vulnerabilities*.
- Devices to which the task will be assigned—you need to assign the task to the root administration group.

- Rules for installing updates:
  - Install approved updates only.
  - Fix vulnerabilities with a severity level equal to or higher than (optional setting).

    If this setting is enabled, updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (*Medium*, *High*, or *Critical*). Vulnerabilities with a severity level lower than the selected value are not fixed.
- Scheduled start—the task run schedule.

For details on how to create a task, please refer to the *Kaspersky Security Center Help Guide*.

> The *Install required updates and fix vulnerabilities* task is available with a Vulnerability and Patch Management license.

Next, you need to install updates for third-party applications and fix vulnerabilities on assets in KUMA.

To install updates and fix vulnerabilities in third-party applications on an asset in KUMA:

1. Open the asset details window in one of the following ways:
   - In the KUMA web interface, select **Assets** → select a category with the relevant assets → select an asset.
   - In the KUMA web interface, select **Alerts** → click the link with the relevant alert → select the asset in the **Related endpoints** section.
   - In the KUMA web interface, select **Events** → search and filter events → select the relevant event → click the link in one of the following fields: SourceAssetID, DestinationAssetID, or DeviceAssetID.
2. In the asset details window, expand the list of **Kaspersky Security Center vulnerabilities**.
3. Select the check boxes next to the applications that you want to update.
4. Click the **Upload updates** link.
5. In the opened window, select the check box next to the ID of the vulnerability that you want to fix.
6. If **No** is displayed in the **EULA accepted** column for the selected ID, click the **Approve updates** button.
7. Click the link in the **EULA URL** column and carefully read the text of the End User License Agreement.
8. If you agree to it, click the **Accept selected EULAs** button in the KUMA web interface.

   The ID of the vulnerability for which the EULA was accepted shows **Yes** in the **EULA accepted successfully** column.
9. Repeat steps 7–10 for each required vulnerability ID.
10. Click the **OK** button.

Updates will be uploaded and installed on the assets managed by the Administration Server where the task was started, and on the assets of all secondary Administration Servers.

> The terms of the End User License Agreement for updates and vulnerability patches must be accepted on each secondary Administration Server separately.

Updates are installed on assets where the vulnerability was detected.

You can update the list of vulnerabilities for an asset in the asset details window by clicking the **Update** link.

Moving assets to a selected administration group

You can move assets to a selected administration group of Kaspersky Security Center. In this case, the group policies and tasks will be applied to the assets. For more details on Kaspersky Security Center tasks and policies, please refer to the *Kaspersky Security Center Help Guide*.

Administration groups are added to KUMA when the hierarchy is loaded during import of assets from Kaspersky Security Center. First, you need to configure KUMA integration with Kaspersky Security Center.

To move an asset to a selected administration group:

1. Open the asset details window in one of the following ways:
   - In the KUMA web interface, select **Assets** → select a category with the relevant assets → select an asset.
   - In the KUMA web interface, select **Alerts** → click the link with the relevant alert → select the asset in the **Related endpoints** section.
2. In the asset details window, click the **Move to KSC group** button.
3. Click the **Move to KSC group** button.
4. Select the group in the opened window.

   > The selected group must be owned by the same tenant as the asset.

5. Click the **Save** button.

The selected asset will be moved.

To move multiple assets to a selected administration group:

1. In the KUMA web interface, select the **Assets** section.
2. Select the category with the relevant assets.
3. Select the check boxes next to the assets that you want to move to the group.
4. Click the **Move to KSC group** button.

   > The button is active if all selected assets belong to the same Administration Server.

5. Select the group in the opened window.

6. Click the **Save** button.

   The selected assets will be moved.

The specific group of an asset is displayed in the asset details.

> Kaspersky Security Center assets information is updated in KUMA when information about assets is imported from Kaspersky Security Center. This means that a situation may arise when assets have been moved between administration groups in Kaspersky Security Center, but this information is not yet displayed in KUMA. When an attempt is made to move such an asset to an administration group in which it is already located, KUMA returns the **Failed to move assets to another KSC group** error.

Asset audit

KUMA can be configured to generate asset audit events under the following conditions:

- Asset was added to KUMA. The application monitors manual asset creation, as well as creation during import via the REST API and during import from Kaspersky Security Center or KICS/KATA.
- Asset parameters have been changed. A change in the value of the following asset fields is monitored:
  - Name
  - IP address
  - MAC address
  - FQDN
  - Operating system

  Fields may be changed when an asset is updated during import.
- Asset was deleted from KUMA. The application monitors manual deletion of assets, as well as automatic deletion of assets imported from Kaspersky Security Center and KICS/KATA, whose data stopped coming.
- Vulnerability info was added to the asset. The application monitors the appearance of new vulnerability data for assets. Information about vulnerabilities can be added to an asset, for example, when importing assets from Kaspersky Security Center or KICS/KATA.
- Asset vulnerability was resolved. The application monitors the removal of vulnerability information from an asset. A vulnerability is considered to be resolved if data about this vulnerability is no longer received from any sources from which information about its occurrence was previously obtained.
- Asset was added to a category. The application monitors the assignment of an asset category to an asset.
- Asset was removed from a category. The application monitors the deletion of an asset from an asset category.

By default, if asset audit is enabled, under the conditions described above, KUMA creates not only audit events (`Type = 4`), but also base events (`Type = 1`).

Asset audit events can be sent to storage or to correlators, for example.

Configuring an asset audit

To configure an asset audit:

1. In the KUMA web interface, open **Settings** → **Asset audit**.

2. Perform one of the following actions with the tenant for which you want to configure asset audit:

   - Add the tenant by using the **Add tenant** button if this is the first time you are configuring asset audit for the relevant tenant.

     In the opened **Asset audit** window, select a name for the new tenant.

   - Select an existing tenant in the table if asset audit has already been configured for the relevant tenant.

     In the opened **Asset audit** window, the tenant name is already defined and cannot be edited.

   - Clone the settings of an existing tenant to create a copy of the conditions configuration for the tenant for which you are configuring asset audit for the first time. To do so, select the check box next to the tenant whose configuration you need to copy and click **Clone**. In the opened **Asset audit** window, select the name of the tenant to use the copied configuration.

3. For each condition for generating asset audit events, select the destination to where the created events will be sent:

   a. In the group of settings for the relevant type of asset audit events, use the **Add destination** drop-down list to select the type of destination to which you want to send the created events:

      - Select **Storage** if you want events to be sent to storage.

      - Select **Correlator** if you want events to be sent to the correlator.

      - Select **Other** if you want to select a different destination.

        > This type of resource includes correlator and storage services that were created in previous versions of the solution.

      In the **Add destination** window that opens you must define the settings for event forwarding.

   b. Use the **Destination** drop-down list to select an existing destination or select **Create** if you want to create a new destination.

      If you are creating a new destination, fill in the settings as indicated in the destination description.

   c. Click **Save**.

   A destination has been added to the condition for generating asset audit events. Multiple destinations can be added for each condition.

4. Click **Save**.

   The asset audit has been configured. Asset audit events will be generated for those conditions for which destinations have been added. Click **Save**.

Storing and searching asset audit events

Asset audit events are considered to be base events and do not replace audit events. Asset audit events can be searched based on the following parameters:

Event field	Value
DeviceVendor	`Kaspersky`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Enabling and disabling an asset audit

You can enable or disable asset audit for a tenant:

To enable or disable an asset audit for a tenant:

1. In the KUMA web interface, open the **Settings** → **Asset audit** section and select the tenant for which you want to enable or disable asset audit.

   The **Asset audit** window opens.

2. Select or clear the **Disabled** check box in the upper part of the window.

3. Click **Save**.

By default, when asset audit is enabled in KUMA, when an audit condition occurs, two types of events are simultaneously created: a base event and an audit event.

You can disable the generation of base events with audit events.

To enable or disable the creation of base events for an individual condition:

1. In the KUMA web interface, open the **Settings** → **Asset audit** section and select the tenant for which you want to enable or disable a condition for generating asset audit events.

   The **Asset audit** window opens.

2. Select or clear the **Disabled** check box next to the relevant conditions.

3. Click **Save**.

For conditions with the **Disabled** check box selected, only audit events are created, and base events are not created.

Detection of unknown assets

By processing events, KUMA lets you detect unknown assets in the infrastructure that are not included in the list of added KUMA assets. The asset must have an IP address or host name. An unknown asset being detected can be normal or it may indicate an information security incident.

The following predefined correlation rules are used to detect unknown assets:

- [OOTB][Net] Detection unknown assets in device fields.
- [OOTB][Net] Detection unknown assets in source fields.
- [OOTB][Net] Detection unknown assets in destination fields.

These correlation rules use filters to configure the monitored network segment and exclusion filters. You can use filters to customize the rule logic that suits your particular network infrastructure. Triggered rules add detected unknown assets to the "[OOTB][Net] Detection unknown assets" list.

The "[OOTB][Net] Detection unknown assets" active list retains a record about a detected asset for 7 days. If any rule is triggered again, no duplicate record about the previously added asset is added to the active list.

Correlation rules, filters, and active list are predefined. You can also import these resources from the repository.

Correlation rules

[OOTB][Net] Detection unknown assets in device fields

This rule analyzes the data in the DeviceAddress and DeviceHostName fields of events. If the IP address or host name from these fields is not found in the list of KUMA assets, the rule is triggered.

The following conditions must be satisfied for the rule to trigger:

- The asset is not included in the "[OOTB][Net] Exceptions from the device addresses" exclusion filter.
- The IP address belongs to a subnet specified in the "[OOTB][Net] Controlled network device" filter.

[OOTB][Net] Detection unknown assets in source fields

This rule analyzes the data in the SourceAddress and SourceHostName fields of events. If the IP address or host name from these fields is not found in the list of KUMA assets, the rule is triggered.

The following conditions must be satisfied for the rule to trigger:

- The asset is not included in the "[OOTB][Net] Exceptions from the source addresses" exclusion filter.
- The IP address belongs to a subnet specified in the "[OOTB][Net] Controlled network source" filter.

[OOTB][Net] Detection unknown assets in destination fields

This rule analyzes the data in the DestinationAddress and DestinationHostName fields of events. If the IP address or host name from these fields is not found in the list of KUMA assets, the rule is triggered.

The following conditions must be satisfied for the rule to trigger:

- The asset is not included in the "[OOTB][Net] Detection unknown assets in destination fields" exclusion filter.
- The IP address belongs to a subnet specified in the "[OOTB][Net] Detection unknown assets in destination fields" filter.

Filters

Exclusion filters

Exclusion filters contain lists of IP addresses and host names of assets which prevent correlation rules from triggering when detected. Add IP addresses and host names to exclusion filters before using correlation rules. For the rules to work correctly, filters must not be empty.

Exclusion filters include:

- [OOTB][Net] Exceptions from the device addresses.
- [OOTB][Net] Exceptions from the source addresses.
- [OOTB][Net] Exceptions from the destination addresses.

Exclusion filters are located in the OOTB/Integration directory.

Monitored subnet filters

Subnet filters contain lists of subnets which correlation rules monitor for new assets. Add subnets to filters before using correlation rules. Without a list of subnets, correlation rules are never triggered.

Subnet filters include:

- [OOTB][Net] Controlled network device.
- [OOTB][Net] Controlled network source.
- [OOTB][Net] Controlled network destination.

Subnet filters are located in the OOTB/Integration directory.

Configuring the detection of unknown assets in your network

To configure the detection of unknown assets:

1. In the KUMA web interface, go to the **Resources** → **Filters** section.
2. In the list of filters, select the following filters one by one and specify the IP addresses or host names that you want to exclude from correlation rules:
   - [OOTB][Net] Exceptions from the device addresses.
   - [OOTB][Net] Exceptions from the source addresses.
   - [OOTB][Net] Exceptions from the destination addresses.

3. In the list of filters, select each of the following filters one by one and specify the subnets that you want to be monitored for unknown assets:

   - [OOTB][Net] Controlled network device.
   - [OOTB][Net] Controlled network source.
   - [OOTB][Net] Controlled network destination.

   Unknown asset detection is configured for the specified subnets. Information about detected assets will be added to the "[OOTB][Net] Detection unknown assets" active list.

Custom asset fields

In addition to the existing fields of the asset data model, you can create custom asset fields. Data from the custom asset fields is displayed when you view information about the asset. Custom fields can be filled in with data either manually or using the API.

You can create or edit the custom fields in the KUMA web interface in the **Settings** → **Assets** section, in the **Custom fields** table. The table has the following columns:

- **Name** – the name of the custom field that is displayed when you view information about the asset.
- **Default value** – the value that is written to the custom field when an asset is added to KUMA.
- **Mask** – a regular expression to which the value in the custom field must match.

To create a custom asset field:

1. In the KUMA web interface, in the **Settings** → **Assets** section, click the **Add field** button.

   An empty row is added to the **Custom fields** table. You can add multiple rows with the custom field settings at once.

2. Fill in the columns with the settings of the custom field:

   - **Name** (required)–from 1 to 128 characters in Unicode encoding.
   - **Default value**–from 1 to 1,024 Unicode characters.
   - **Mask**–from 1 to 1,024 Unicode characters.

3. Click **Save**.

   A custom field is added to the asset data model.

To delete or edit a custom asset field:

1. In the KUMA web interface, open **Settings** → **Assets**.
2. Make the necessary changes in the **Custom fields** table:
   - To delete a custom field, click the ✕ icon next to the row with the settings of the required field. Deleting a field also deletes the data written in this field for all assets.
   - You can change the values of the field settings. Changing the default value does not affect the data written in the asset fields before.
   - To change the display order of the fields, drag the rows by the ⠿ icon
3. Click **Save**.

   The changes are made.

Critical information infrastructure assets

In KUMA, you can tag assets related to the critical information infrastructure (CII) of the Russian Federation. This allows you to restrict the KUMA users capabilities to handle alerts and incidents, which are associated with the assets related to the CII objects.

> You can assign the CII category to assets if the license with the GosSOPKA module is active in KUMA.

General administrators and users with the **Access to CII facilities** check box selected in their profiles can assign the CII category to an asset. If none of these conditions are met, the following restrictions apply to the user:

- The **CII category** group of settings is not displayed in the **Asset details** and **Edit asset** windows. You cannot view or change the CII category of an asset.
- Alerts and incidents associated with the assets of the CII category are not available for viewing. You cannot perform any actions on such alerts and incidents; they are not displayed in the table of alerts and incidents.
- The **CII** column is not displayed in the Alerts and Incidents tables.
- Search and closing of the alerts using the REST API is not available.

The CII category of an asset is displayed in the **Asset details** window in the **CII category** group of settings.

To change the CII category of an asset:

1. In the KUMA web interface, in the **Assets** section, select the required asset.

   The **Asset details** window opens.

2. Click the **Edit** button and select one of the available values in the drop-down list:

   - **Information resource is not a CII object** – default value, indicating that the asset does not have a CII category. The users with the **Access to CII facilities** check box cleared in their profiles can work with such assets and the alerts and incidents related to these assets.
   - **CII object without a significance category**.
   - **CII object of the third category of significance**.
   - **CII object of the second category of significance**.
   - **CII object of the first category of significance**.

3. Click **Save**.

Storing confidential information (secrets)

Secrets are used to securely store confidential information, such as user name and password, that Kaspersky SIEM uses to interact with external services. If a secret stores account data such as user login and password, when the collector connects to the event source, the user account specified in the secret may be blocked in accordance with the password policy configured in the event source system.

Secrets can be used in collectors and connectors when using TLS encryption, in destinations when using TLS encryption or authorization, and for proxies.

Viewing secrets

To view secrets,

In the web interface, go to the **Resources and services** → **Secrets** section.

The secrets table opens.

A secret created inside a resource in the Shared tenant is not displayed in the **Resources and services** → **Secrets** section and is not viewable, even by a user with the General Administrator role. Such a secret can be viewed and managed within the resource in which it was created, and is available only for viewing in the **Resources and services** section when the **List** display type is selected.

You can use the **Search** field to search for secrets by their names. Regular expressions are used when searching for secrets.

You can sort the table by name, type, last update time, or package name by clicking the sort icon ⌄ in the column header and selecting either **Ascending** or **Descending**.

The secrets table contains the following columns:

- **Name** is a secret name.
- **Type**—the type of a secret. To search for types, click the sorting icon in the column header, and specify a value to search for in the **Search** field or select types using check boxes.
- **Resource path** is the tenant that owns the secret.
- **Updated** is the date and time of the last update of a secret.
- **Created by** is the name of a user who created a secret.
- **Description** is optional information about the secret.
- **Tags** serve for secret searching. To search for secrets by tags, click the sort icon in the column header, and specify a value to search for in the **Search** field or select tags using check boxes.
- **Package name** is the name of the package of tools for processing events.

Creating a secret

To create a secret:

1. In the web interface, go to the **Resources and services** → **Secrets** section.
2. In the toolbar or menu ⋮, click the **Create** button.
3. This opens a sidebar; in the sidebar, in the **Name** field, enter a unique name for the secret. The name must contain 1 to 128 Unicode characters.
4. In the **Tenant** drop-down list, select the tenant that will own this secret.
5. In the **Type** drop-down list, select the type of enrichment rule and configure the settings specific to the selected secret type:

   credentials

   A secret of **credentials** type is used to store account data for connecting to external services such as SMTP servers or database management systems (DBMS). For example, when a secret of **credentials** type is used to connect a collector to an event source, the account defined in the secret is blocked if it violates the password policy configured for the event source.

   If you select this type of secret, fill in the **User** and **Password** fields.

   When changing a previously saved secret of the credentials type, the user name and password fields are displayed empty. The values of these fields are preserved, you do not need to enter them again.

   token

   A secret of **token** type is used to store tokens for API requests. Tokens are used when connecting to IRP systems, for example.

   If you select this type of secret, fill in the **Token** field.

ktl

ktl secret is used to store Kaspersky Threat Intelligence Portal account credentials.

If you select this type of secret, do the following:

1. In the **User** and **Password** fields, enter user name and password of your Kaspersky Threat Intelligence Portal account.

2. To upload a Kaspersky Threat Intelligence Portal certificate key, click the **PFX file** button.

3. In **PFX password** field, enter the password for accessing the Kaspersky Threat Intelligence Portal certificate key.

urls

urls secret is used to store URLs for connecting to SQL databases and proxy servers.

If you select this type of secret, fill in the **URL** field. You can specify URLs in the following formats: hostname:port, IPv4:port, IPv6:port, :port.

In the **Description** field, you should provide a description of the connection for which you are using the secret of **urls** type.

pfx

pfx secret is used for importing a PFX file containing certificates.

If you select this type of secret, do the following:

1. Click the **Personal Information Exchange—PKCS (.PFX)** button to upload the PFX file.

   The file must contain a certificate and key. PFX files may include CA-signed certificates for server certificate verification.

   > The certificate included in the PFX file cannot be encrypted with the AES-128-CBC algorithm. Kaspersky SIEM does not support such certificates.

2. In the **PFX password** field, specify the password for accessing the certificate key.

kata/edr

kata/edr secret is used to store the certificate file and private key required when connecting to the Kaspersky Endpoint Detection and Response server.

If you select this type of secret, in the **Authentication files** section, do the following:

1. If necessary, generate a certificate and a private encryption key.

2. Click the **Upload certificate** button and upload the KUMA server certificate.

   The file must be in PEM format. You can upload only one certificate file.

3. Click the **Upload private key** button and upload the RSA key file of the KUMA server.

   The key must be without a password and with the PRIVATE KEY header. You can upload only one key file.

snmpV1/V2

snmpV1/V2 secret is used to store the values of **Community** (for example, `public` or `private`) required for interaction over the Simple Network Management Protocol.

If you select this type of secret, fill in the **Community** field.

snmpV3

The **snmpV3** secret is used to store data required for communication over the Simple Network Management Protocol.

If you select this type of secret, do the following:

1. In the **User** field, enter a user name without a domain.
2. In the **Security Level** drop-down list, select one of the following options:
   - **NoAuthNoPriv**—messages are forwarded without authentication and confidentiality measures.
   - **AuthNoPriv**—messages are forwarded with authentication but without confidentiality measures.
   - **AuthPriv**—messages are forwarded with authentication and ensured confidentiality.
3. If you select **AuthNoPriv** or **AuthPriv** option, enter the SNMP user authentication password in the **Password** field.
4. If you select the **AuthNoPriv** or **AuthPriv** option, in the **Authentication Protocol** drop-down list, select the required protocol: MD5, SHA, SHA224, SHA256, SHA384, or SHA512.
5. If you select the **AuthPriv** option, in the **Privacy Protocol** drop-down list, select the required protocol: DES or AES.
6. If you select the **AuthPriv** option, in the **Privacy password** field, enter the encryption password that was set when the SNMP user was created.

certificate

certificate secret is used for storing certificate files.

If you select this type of secret, upload the certificate by clicking the **Upload certificate file** button. X.509 certificate public keys in Base64 are supported.

fingerprint

fingerprint secret is used to store the **Elastic fingerprint** parameter value that can be used when connecting to the Elasticsearch server.

If you select this type of certificate, fill in the **Elastic fingerprint** field.

PublicPKI

The secret of the **PublicPKI** type is used to connect the collector to ClickHouse.

If you select this option, you must specify the secret containing the base64-encoded PEM private key and the public key.

ssh private key

A secret of the **ssh private key** type is used in the SFTP connector to connect to the SFTP server.

If you select this option, you need to specify a user name and a file containing the SSH private key.

6. If necessary, select the tags for the secret from the **Tags** drop-down list.

7. If required, add a description for the secret in the **Description** field. Description can contain up to 4,000 Unicode characters.

8. Then click the **Create** button.

The secret is saved and displayed in the table.

Deleting a secret

To delete a secret:

1. In the web interface, open the **Resources and services** section and select the **List** display type for resources and services.

   The **List** mode displays all secrets, including built-in secrets created in the resources of the Shared tenant. Such secrets are not displayed in the **Secrets** section.

2. If a secret is linked to a resource, unlink it in one of the following ways before deleting it:

   - In the resource, select another secret. This automatically unlinks the current secret and makes it available for deletion.

   - Delete the resource to which the secret is linked. This also automatically unlinks the secret and makes it available for deletion.

3. In the list, select the check box next to the secret that you want to delete, and in the toolbar, click **Delete**.

The secret is deleted.

Predefined secrets

The secrets listed in the table below are included in the Kaspersky SIEM distribution kit.

Predefined secrets

Secret name	Description
[OOTB] Continent SQL connection	Stores confidential data and settings for connecting to the APKSh Kontinent database system. To use it, you must specify the login and password to the database.
[OOTB] InfoWatch Person Monitor MS SQL connection	Stores confidential data and settings for connecting to the MS SQL database of the InfoWatch Person Monitor system. To use it, you must specify the login and password to the database.
[OOTB] InfoWatch Traffic Monitor SQL Connection	Stores confidential data and settings for connecting to the database of the InfoWatch Traffic Monitor system. To use it, you must specify the login and password to the database.
[OOTB] Kaspersky Security for Exchange SQL connection	Stores confidential data and settings for connecting to the database of the Kaspersky Security for Microsoft Exchange Servers system. To use it, you must specify the login and password to the database.
[OOTB] KSC MS SQL connection	Stores confidential data and settings for connecting to the MS SQL database of Kaspersky Security Center. To use it, you must specify the login and password to the database.

Secret name	Description
[OOTB] KSC MySQL Connection	Stores confidential data and settings for connecting to the MySQL database of Kaspersky Security Center. To use it, you must specify the login and password to the database.
[OOTB] KSC PostgreSQL connection	Stores confidential data and settings for connecting to the PostgreSQL database of Kaspersky Security Center. To use it, you must specify the login and password to the database.
[OOTB] Oracle Audit Trail SQL Connection	Stores confidential data and settings for connecting to the Oracle system database. To use it, you must specify the login and password to the database.
[OOTB] Parsec MSSQL connection	Stores confidential data and settings for connecting to the MS SQL database of the Parsec system. To use it, you must specify the login and password to the database.
[OOTB] SecretNet SQL connection	Stores confidential data and settings for connecting to the MS SQL database of the SecretNet system. To use it, you must specify the login and password to the database.
[OOTB] TeamPass MySQL connection	Stores confidential data and settings for connecting to the MySQL database of the TeamPass system. To use it, you must specify the login and password to the database.
[OOTB] Zabbix audit MySQL	Stores confidential data and settings for connecting to the MySQL database of the Zabbix system. To use it, you must specify the login and password to the database.

Working with the knowledge base

For a more hands-on experience with managing packages and resources provided by Kaspersky, Kaspersky SIEM has the Knowledge Base section.**Knowledge base** In this section, you can view available and installed packages and resources, install individual resources or whole packages, evaluate the coverage of MITRE ATT&CK techniques with installed resources, check if the resources are up to date, search and filter by specified criteria.

Packages contain sets of resources for configuring Kaspersky SIEM. Packages can be downloaded from the Kaspersky repository.

> If no packages from the repository have been downloaded thus far, the list of packages and resources in the **Knowledge base** section is empty. To get the packages and resources available for installation, you need to configure updates for preinstalled resources.

Viewing information about packages and resources

To open the Knowledge Base:

In the web interface of the solution, go to the **Resources** → **Knowledge base** section.

This section contains widgets that display summary information about packages and resources in your KUMA instance. You can show or hide widgets by clicking the view widget icon . The following widgets are available:

- **Package status** is the number of packages with the following statuses:
  - **Available** means the package is available for installation.
  - **Installed** means the whole package is installed.
  - **Emergency** means the package contains high-priority resources that need to be installed as soon as possible.

- **New** means the package was added to the repository less than three months ago and has not yet been installed or viewed.
- **Update required** means a newer version is available for the package in the repository.

  To update a package, you need to reinstall the package. Reinstalling installs the currently available version of the package.

- **Resource status** is the number of resources of various types with the following statuses:
  - **Available** means the resource is available for installation.
  - **Installed** means the resource is installed and does not need an update.
  - **Update required** mean a newer version is available for the resource in the repository.
- **MITRE Technique Coverage, {{ filter }}** provides information about the number or MITRE ATT&CK techniques covered or coverage percentage by the selected resources.

Widgets also act as filters for tables on the page. When you select a value in a widget, the table is automatically updated in accordance with the selected filter. For example, you can display only resources with the **Update required** status.

When managing the table, you can use the **Packages** and **Resources** tabs.

Description of the Packages tab

The **Packages** tab displays a table of available packages, which contains the following columns:

- **Name** is the name of the package.
- **Version** is the version of the package.
- **Release date** is the date when the package was released.
- **Resource kinds** are types of resources included in the package:
  - Active list
  - Context table
  - Normalizer
  - Event aggregation rule
  - Correlation rule
  - Enrichment rule
  - Dictionary
  - Filter
  - Notification template
- **Number of resources** is the number of resources in the package.

- **Status** is the status of the package.
  - **Available** means the package is available for installation.
  - **Installed** means the whole package is installed.
  - **Emergency** means the package contains high-priority resources that need to be installed as soon as possible.
  - **New** means the package is new and available for installation.
  - **Update required** means a newer version is available for the package in the repository.

    To update a package, you need to reinstall the package. Reinstalling installs the currently available version of the package.
- **Description** is a description of the package.

To view information about a package, click its name. This opens a window with information about the package, which contains the **General** and **Change log** tabs.

The following information is displayed on the **General** tab:

- Package name
- Description
- Release date
- Version

This tab also contains the **Resources to be imported** section, which displays a list of resources included in the package. Here you can filter the resources and select only those that you need to install.

The **Change log** tab displays information about changes made to the package, including changes of any resources included in the package. Changes are grouped by package release dates.

Description of the Resources tab

The **Resources** tab displays a table of available resources, which contains the following columns:

- **Name**—the name of the resource.
- **Resource kind**—available types of resources:
  - Active list
  - Context table
  - Normalizer
  - Event aggregation rule
  - Correlation rule
  - Enrichment rule

- Dictionary
- Filter
- Notification template

- **Installation date** is the date when the resource was installed in KUMA.
- **Tenant** is the tenant in which the resource is installed.

  If the same resource is installed for several tenants, it is displayed in the table as a group. To view the details of the resource in each tenant for which it is installed, expand the group.
- **Version** is the version of the resource.
- **Status** is the status of the resource.
  - **Available** means the resource is available for installation.
  - **Installed** means the resource is installed.
  - **Update required** mean a newer version is available for the resource.
- **Package names** lists packages that include this resource.
- **Vendor tags** are tags assigned by the vendor of the resource.
- **MITRE Techniques** are MITRE ATT&CK techniques associated with the resource.

To view information about a resource, click its name. This opens the resource information window, which contains the **General info** and **Linked resources** tabs.

On the **Linked resources** tab, you can view the resources linked to the selected resource. You can also view dependencies on the **Resources** tab by clicking the **Show dependencies** button.

You can use the **Search** field to search for packages or resources. The search is performed only on the currently opened tab. When you switch between tabs, the entered search query is kept and applied to the selected tab. In the **Search** field, you can enter the resource name, event source, event type, package name, or any substring.

To filter the contents of the **Packages** and **Resources** tabs, click the filter icon.

You can sort the tables by clicking the column header of the relevant parameter and selecting **Ascending** or **Descending**. You can also filter the table by the **Resource kind** or **Status** columns by clicking the relevant column's heading and selecting the values that need to be displayed.

About package and resource import

Resources are imported to the selected tenant. Resources linked to the Shared tenant will be imported into the Shared tenant. The account does not require permissions in the Shared tenant. Only import permissions are required in the selected tenant.

Imported OOTB resources cannot be modified or moved. If you want to modify or move an imported OOTB resource, create a copy of it. When importing subsequent versions of the package, the copy is not updated because it is a separate object.

You can edit imported resources in the `Integration` folder. Such resources are marked as **This resource is a part of the package** You can add a dictionary of `Table` type to a package resource in the `Integration` folder. You cannot add other types of resources. When importing subsequent versions of the package, the edited resource will not be replaced with the corresponding resource from the package, which allows you to keep the changes you made.

Resources from the repository are imported from the repository in the language specified in the **KUMA resources localization** setting in the KUMA Core settings section.

Installing packages

A package gets the **Installed** status only if all resources it includes are installed.

To install the whole package:

1. Go to the **Resources** → **Knowledge base** → **Packages** section.
2. Do one of the following:
   - Select the check box next to the relevant package and click the **Install** button.
   - Click the name of the package to open a window, and in that window, click the **Install** button.
3. Select a tenant.
4. Click the **Install** button.

   The resources are imported into KUMA and become available for further configuration.

Installing individual resources

To install individual resources from a package:

1. Go to the **Resources** → **Knowledge base** → **Resources** section.
2. Do one of the following:
   - Select the check box next to the relevant resources and click the **Install** button.
   - Click the name of the resource to open a window, and in that window, click the **Install** button.
3. Select a tenant.
4. Click the **Install** button.

   The resource is installed.

Updating resources

If a new version is available for an installed resource, the resource gets the **Update required** status.

To update a resource:

1. Go to the **Resources** → **Knowledge base** → **Resources** section.
2. Select the check box next to one or more resources with the **Update required** status.
3. Click the **Update** button.

Managing resources and services

The main components of Kaspersky SIEM used for managing events are *services*. Services receive events from data sources and normalize them into a unified format for correlation search, storage, and manual analysis. An identifier is assigned to each service upon creation.

The following types of services are available in Kaspersky SIEM:

- Storages are used to save events.
- Correlators are used to analyze events and search for defined patterns.
- Collectors are used to receive events and convert them to KUMA format.
- Agents are used to receive events on remote devices and forward them to collectors.
- Event routers receive streams of events from collectors and correlators and then distribute the events to destinations in accordance with the configured filters.

Services are created based on *resources*. Resources are components of Kaspersky SIEM that contain parameters for implementing various functions, for example, to establish a connection to a specific URL or convert data according to specific rules. Resources can be grouped into resource sets. When resources are grouped in a set, they must be owned by the same tenant that owns the created resource set. An exception is the Shared tenant, whose owned resources can be used in the sets of resources of other tenants.

Kaspersky SIEM comes with a set of predefined resources. The predefined resources contain the **[OOTB]** prefix in their names. Such resources cannot be modified. However, you can create a copy of the predefined resource and modify the copy.

Some resources are linked to each other. For example, in certain types of connectors, you must specify the secret of the connector. When importing or exporting such connectors, the linked secrets are also imported or exported.

In Kaspersky SIEM, you can create the following types of resources:

- **Correlation rules**—resources of this type contain rules for identifying event patterns that indicate threats. If the conditions specified in these resources are met, a correlation event is generated.
- **Normalizers**—resources of this type contain rules for converting incoming events into the format used by Kaspersky SIEM. After processing in the normalizer, the "raw" event becomes normalized and can be processed by other resources and services.
- **Connectors**—resources of this type contain settings for establishing network connections.
- **Aggregation rules**—resources of this type contain rules for combining several basic events of the same type into one aggregation event.
- **Enrichment rules**—resources of this type contain rules for supplementing events with information from third-party sources.
- **Destinations**—resources of this type contain settings for forwarding events to a destination for further processing or storage.
- **Filters**—resources of this type contain criteria for selecting individual events from the event stream to be sent to processing.
- **Response rules**—resources of this type are used in correlators to, for example, execute scripts or launch Kaspersky Security Center tasks when certain conditions are met.
- **Segmentation rules**—resources of this type are used in correlators to separate same-type correlation events into different alerts.
- **Data collection and analysis rules**—resources of this type contain rules that allow scheduling SQL queries with aggregation functions to the storage. Data received from SQL queries is then used for correlation.
- **Notification templates**—resources of this type are used when sending notifications about new alerts.
- **Active lists**—resources of this type are used by correlators for dynamic data processing when analyzing events according to correlation rules.
- **Dictionaries**—resources of this type are used to store keys and their values, which may be required by other KUMA resources and services.
- **Proxies**—resources of this type contain settings for using proxy servers.
- **Secrets**—resources of this type are used to securely store confidential information (such as credentials) that KUMA needs to interact with external services.
- **Context tables**—resources of this type are used by KUMA correlators to analyze events in accordance with correlation rules.
- **Dashboards** are used to monitor the security status of the corporate network. The dashboard is a set of widgets that display security data analytics.
- **Report templates** are used to configure the periodic generation of reports on the status of processes and objects in the corporate network. The template specifies the request, data display parameters, and the schedule for report generation.

Resources and services are located in folders that you can add, rename, move, and delete.

General instructions for working with resources

This section provides general instructions for working with resources.

To view the resource table:

in the web interface, go to the **Resources** → **<resource type>** section.

The table of the selected resource opens.

You can use the **Search** field to search for resources by their names. Regular expressions are used when searching for resources.

You can sort the table by name, date and last update time, or tags by clicking the sort icon ⌄ in the column header and selecting either **Ascending** or **Descending**.

The resource table contains the following columns:

- **Name**—the name of the resource.
- **Updated**—the date and time of the last update of a resource.
- **Created by**—the name of the user who created a resource.
- **Description**—the description of a resource.
- **Type**—the type of the resource. Displayed for all types of resources, except **Aggregation rules**, **Enrichment rules**, **Data collection and analysis rules**, **Filters**, **Active lists**, **Proxies**.
- **Resource path**—folder in the resource tree.
- **Tags**—tags assigned to the resource. A resource can have more than one tag. Tags are part of the resource and are imported with the resource.
- **Package name**—the name of the package in which the resource was imported from the repository.
- **Correlator**—list of correlators to which the correlation rule is linked. Displayed only for resources of the **Correlation rule** type.

  For a rule that is not linked to any correlator, the column is blank. If the list contains multiple values, these values are sorted alphabetically. You can filter the values in the **Correlator** column by clicking the column header and selecting the correlation rules that you want to view in the table: **Without correlator** or **With correlator**.

  For rules of the Shared tenant, the correlators of tenants to which you have access and which you selected in the tenant list are displayed.

  Values in the **Correlator** column are not editable. If you want to perform actions on correlators, you need to click the rule in the table to open the properties of the rule, and go to the **Correlators** tab.
- **MITRE techniques**—the MITRE matrix techniques that this correlation rule covers. Displayed only for resources of the **Correlation rule** type. When you hover over a value, the name of the rule is displayed.

If necessary, you can customize the columns by clicking the gear ⚙ icon.

The maximum table size is not limited. If you want to select all resources, scroll to the end of the table and select the **Select all** check box, which selects all available resources in the table.

The table of resources in the lower part displays the number of resources from tenants that are available to you in the table:

- **Total** is the total amount or the amount with the filter or search applied.
- **Selected** is the number of selected resources.

When filters are applied, the resource selection and the **Selected** value are reset. If the amount of resources changes due to the actions (for example, deletion) undertake by another user, the displayed number of resources changes after you refresh the page, perform an action with the resource, or apply a filter.

Creating, duplicating, moving, editing, and deleting resources

This article describes how to change, copy, and delete a resource.

Editing a resource

To edit the resource:

1. In the **Resources** → **<resource type>** section, click the resource that you want to edit.

   On the right side, a pane with the settings of the selected resource opens. Parameters depend on the resource type.

2. Make the necessary changes.

3. Save changes:

   - Click **Save** to save your changes.
   - Click **Save with comment**, and in the window that opens add a comment that describes your changes. The comment will be added to the created version of the resource.

   The resource is changed, and a new version is created for it. If this resource is used in a service, restart the service to apply the new version of the resource.

   If the current resource is not editable (for example, you cannot edit correlation rules), you can go to the card of another resource by clicking the **View** button. This button becomes available in batch resources when you click another resource linked to the current resource.

If, when saving a resource, it turns out that the current version of the resource has been modified by another user, you will have one of the following options:

- Save your changes as a new version of the resource on top of the changes made by the other user.
- Save your changes as a new resource.

  In this case, a duplicate of the original resource is created with the changed settings. The `- copy` string is added to the name of the new resource, and the name and version of the duplicated resource are specified in the version comments.
- Discard your changes.

  Discarded changes cannot be restored.

Creating a resource based on an existing one

To create a copy of the resource:

1. In the **Resources** → **<resource type>** section, select the check box next to the resource that you want to copy.

   You can copy only one resource at a time.
2. In the toolbar or in the menu (⋮), click **Duplicate**.

   This opens a pane with the settings of the selected resource. The available configuration parameters depend on the resource type.
3. If necessary, change the name of the resource in the **Name** field.

   By default, the field displays `<name of the selected resource> - copy`.
4. Make the necessary changes to the parameters.
5. Click **Create**.

The resource is created based on the existing one.

Deleting a resource

To delete the resource:

1. In the **Resources** → **<resource type>** section, select the check boxes next to one or more resources that you want to delete.

   To select multiple resources at the same time, select the check box in the header of the first column and select one of the following options:

   - **Select all** selects all resources on all pages of the table. If resources are filtered using search, all resources that match the search condition are selected.
   - **Select all in page** selects all resources on the currently opened page. If resources are filtered using search, all resources on the opened page that match the search condition are selected.

The number of selected resources is displayed in the lower part of the table.

2. In the toolbar or in the menu (⋮), click **Delete**.

   This opens a window that tells you whether it is safe to delete resources, depending on whether the resources selected for deletion are linked to other resources.

   For resources that cannot be deleted, existing links are displayed in a table.

3. Confirm resource deletion.

Resources without links and all saved versions of these resources are deleted.

Linking resources to services

You can now link correlation rules, enrichment rules, response rules, aggregation rules, and destinations to services such as collectors, correlators, and event routers. The available services depend on the type of the selected resource.

To link a resource to a service:

1. In the web interface, open the **Resources** → **<resource name>** section.

2. Select the check boxes next to the resources you want to link.

3. In the toolbar or menu ⋮, click **Link to service** → **Link to <service name>**.

   You can also link a resource to a service when editing resource settings. To do this, click the name of a resource, select the **Services** tab, and click **Link to service** → **Link to <service name>**.

   > When managing the settings of a correlation rule, you can use the **Correlators** tab to link the rule to correlators.

   You can also link a resource when creating or editing service settings. To do so, in the service settings window, go to the section corresponding to the resource type and add the required resource. For example, if you want to link an enrichment rule to a collector, go to the **Event enrichment** section and add a rule by clicking the **Add enrichment** button.

4. In the **<service name>** window that opens, select the check boxes next to the relevant services, and click **OK**.

The resource is linked to the service.

To unlink a resource from a service:

1. In the web interface, open the **Resources** → **<resource name>** section.

2. Click the resource and select the **Services** tab.

   > For correlation rules, the **Correlators** tab is displayed.

   You can also unlink a resource while editing service settings. To do this, in the service settings window, go to the section in which the resource was added and delete it.

3. Select the check boxes next to the services from which you want to unlink the resource.

4. Click **Delete** and confirm the unlinking from the service.

   The resource is unlinked from the service.

Updating predefined resources

KUMA comes with a predefined set of resources, such as normalizers, correlation rules, and connectors. Kaspersky specialists regularly update these resources, for example, add new correlation rules. To use the latest versions of the resources, you need to configure their updates.

In the resource list, predefined resources are marked with the **[OOTB]** prefix. To learn more about updating OOTB resources, watch the video below, then follow the step-by-step scenario.

https://www.youtube.com/watch?v=Epx6BuQBIW8

Updating predefined resources from the repository consists of the following stages:

1. Preparing to update resources

If you plan to download updates directly from Kaspersky update servers, the server with KUMA Core installed must have internet access.

If the server with KUMA Core installed has no internet access, you need to download updates from any computer with internet access using the Kaspersky Update Utility. In this case, the repository is updated from the custom source. You can download the distribution kit from the Kaspersky Technical Support website.

2 Configuring resource updates

Configure resource updates in the repository either from Kaspersky update servers or from a custom source.

1. In the web interface, go to the **Settings** → **Other** → **Update settings** section.

2. In the **Update source** drop-down list, select one of the following options:

   - **Kaspersky update servers**.

     You can view the list of update servers in the Knowledge Base.

   - **Custom source**.

     When downloading updates via a custom source, you can preconfigure the use of the Kaspersky Update Utility, which allows you to update resources without internet access. For detailed information about working with Kaspersky Update Utility, refer to the Kaspersky Knowledge Base.

     How to configure the use of Kaspersky Update Utility

     1. In Kaspersky Update Utility, enable the download of updates for KUMA using one of the following ways:

        - In a drop-down list, select **Application list**, then click the **Select** button. In the window that opens, in the **Perimeter control** section, select the check box next to the version of KUMA you are using.

        - If you work with Kaspersky Update Utility using the command line, add the following line to the `[ComponentSettings]` section of the `updater.ini` configuration file or specify the `true` value for an existing line:

          ```
          KasperskyUnifiedMonitoringAndAnalysisPlatform_4_2=true
          ```

     2. In the **Downloads** section, specify the update source. By default, Kaspersky update servers are used as the update source.

     3. In the **Downloads** section, in the **Update folders** group of settings, specify the shared folder for Kaspersky Update Utility to download updates to.

3. If you selected the **Custom source** option, in the **URL** field specify either the path to a shared folder on an HTTP server or the full path to a local folder on the server with KUMA Core installed.

   If a local folder is used, the system user must have read access to this folder and its contents.

4. If necessary, in the **Proxy server** list, create or select an existing proxy server to be used when running the **Repository update** task.

5. If you want to receive email notifications about new packages or versions of packages that you have previously imported into the tenant, in the **Emails for notification** field, specify the relevant email addresses by clicking the **Add** button.

   To send email notifications, you need to configure a connection to an SMTP server.

   If you specify the email address of a KUMA user, the **Receive email notifications** check box must be selected in the user profile. For emails that do not belong to any KUMA user, the messages are received without additional settings.

6. If you want to enable automatic repository updates:

   a. In the **Repository update** section, disable the **Disable automatic update** toggle switch.

   b. In the **Data refresh interval in hours** field, specify the time in hours. The default value is 24 hours.

7. If you want to start the update manually, click the **Start update** button.

8. Click **Save**.

The update task will start automatically shortly. Subsequently, the task will run in accordance with the schedule.

❸ Importing resources into the tenant

After updating the repository, import the resource packages into the tenant.

❹ Linking resources to services

For the services to start using the updated resources, make sure that they are linked. If necessary, link the resources to collectors, correlators, or agents, and update the settings of the corresponding service.

Exporting resources

> If shared resources are hidden for a user, it is impossible to export shared resources or resources that use the shared resources.

To export resources:

1. In the web interface, in the **Resources** section, click **Export resources**.

   The **Export resources** window opens.

2. In the **Password** field enter the password that must be used to protect exported data.

   Password requirements:

   - At least 16 characters.
   - Must contain uppercase and lowercase letters, numerals, and special characters (for example, @, #, $).
   - May not contain three or more identical characters in a row.

3. In the **Tenant** drop-down list, select the tenant whose resources you want to export.

4. Select the check boxes next to the resources that you want to export.

   If selected resources are linked to other resources, linked resources will be exported, too.

The number of selected resources is displayed in the lower part of the table.

5. Click the **Export** button.

Current versions of resources in a password-protected file are saved on your computer in accordance with your browser settings. Previous versions of the resources are saved in the file. The Secret resources are exported blank.

To export a previous version of a resource:

1. In the web interface, in the **Resources** section, select the relevant type of resources.

   This opens a table with available resources of this type.

   If you want to view all resources, in the **Resources** section, go to the **List** tab.

2. Select the check box next to the resource whose version you want to export.

3. In the toolbar or menu ⋮, click the **View versions history** button.

   This opens the window with the version history of the resource.

4. Click the row of the resource version that you want to export and then click the **Export** button in the lower part of the window.

   > You can only export a previous version of a resource. The **Export** button is not displayed when the current version of the resource is selected.

The resource version is saved in a JSON file on your computer in accordance with your browser settings.

Importing resources

This article describes how to import resources from a file. You can import resources from the repository in the Knowledge base section.

When working with Kaspersky SIEM, we recommend to use resources from the [OOTB] KUMA 4.6 resources package and resources published in the repository after the release of this package.

> Kaspersky SIEM supports importing resources from an earlier version to a later version, for example from KUMA 3.4 to KUMA 4.0.

When importing normalizers, extended event schema fields used in normalizers are automatically created in Kaspersky SIEM. If such a field already exists in the solution, the existing field is used for import.

Extended event schema fields are automatically generated only based on normalizers. For example, when you import a collector that contains normalizers, all the extended schema fields used by the normalizers are automatically created. Fields that are used only in enrichments or correlation rules, but are not used in normalizers are not automatically created in Kaspersky SIEM.

To import resources from a file:

1. In the **Resources** section, click **Import resources**.

   The **Import resources** window opens.

2. In the **Tenant** drop-down list, select the tenant that will own the imported resources.

3. Select the file from which you want to import resources and specify the password for this file.

4. Click **Import**.

5. If there are conflicts between imported from the file and existing resources, the **Conflicts** window is opened. By default, the **Parent object** column displays the top-level parent resource from those selected during import.

   Do the following:

   a. If the name, type, and GUID of a imported resources fully match the name, type, and ID of an existing resource, the **Conflicts** window opens with the table containing the type and the name of the conflicting resources. Resolve displayed conflicts:

      - To replace the existing resource with a new one, click **Replace**.

        To replace all conflicting resources, click **Replace all**. In this case, all related resources are also automatically replaced by the imported resources.

      - To leave the existing resource, click **Skip**.

        The **Skip** option is not available for resources that are linked to other resources. For such resources, you can only select the **Replace** option.

        To keep all existing resources, click **Skip all**.

   b. Click the **Resolve** button.

   The resources are imported into Kaspersky SIEM. The Secret resources are imported blank. In case of a conflict, the imported resources will be added as a new version of the existing resource. A `resources imported` comment is added to this version.

Possible errors

The linked resource is imported into the tenant specified during import, not into the Shared tenant.

Conditions:

- The linked resource is initially located in the Shared tenant.
- In the **Conflicts** window, you select **Skip** for all parent objects of the related resource from the Shared tenant.
- Keep the linked resource from the Shared tenant for replacement.

After import, the tenant is not specified in the category filter.

Conditions:

- The filter contains related asset categories from different tenants.
- Asset category names are the same.
- You are importing this filter with related asset categories to a new server.

In Tenant 1, the name of the asset category is duplicated

Conditions:

- In Tenant 1, you have a filter with related asset categories from Tenant 1 and the Shared tenant.
- Related asset categories have identical names.
- You are importing such filter from Tenant 1 to the Shared tenant.

You cannot import conflicting resources into the same tenant.

The **Impossible to import conflicting resources to the same tenant** error means that the imported package contains conflicting resources from different tenants and cannot be imported into the Shared tenant.

Solution: Select a tenant other than Shared to import the package. In this case, during the import, resources originally located in the Shared tenant are imported into the Shared tenant, and resources from the other tenant are imported into the tenant selected during import.

Only the general administrator can import categories into the Shared tenant.

The **Only the general administrator can import categories into the Shared tenant** error means that the imported package contains resources with related shared asset categories. You can view categories or resources with associated general asset categories in the KUMA Core logs at the following path:

```
/opt/kaspersky/kuma/core/<core_ID>/log
```

where `<core_ID>` is the ID of the KUMA Core instance in Raft. If the KUMA Core is deployed in a single instance, the ID is replaced with zero padding: `/opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000/log`.

Each instance of the KUMA Core has its own log files.

Solution. Do one of the following:

- Do not import resources to which shared categories are linked: clear the check boxes next to the relevant resources.
- Perform the import under a Main administrator account.

Resource search

You can search resources by name or tags. You can also use full-text search to find resources by all their fields. For resources of the **Correlation rules** type, you can use full-text search to search for correlators in which the rules are used. Searching by filter finds all resources that use the filter.

The search is carried out only on the latest version of the resources.

To find resources:

1. In the web interface, in the **Resources** section, select the relevant type of resources.

   This opens a window opens with a table of available resources of this type.

   If you want to view all resources, in the **Resources** section, go to the **List** tab.

2. If necessary, switch the search mode. To do this, click the table icon at the top of the resources table.

   You can search by name, tags, or full-text search in all fields of resources. By default, search by name, tags, and correlators is enabled (only for correlation rules).

   You can tell which search mode is currently enabled by the default text that is displayed in the search field.

3. In the **Search** field, start typing the search text.

   The search is initiated as you type characters in the field and is case-insensitive.

   The table displays only those resources that satisfy the search conditions. The number of such resources is displayed in the lower part of the table.

   For full-text search, the results are sorted in the descending order of the number of words from the search string found in the fields of a resource. KUMA performs a search by the resource JSON. If a different resource is specified in the JSON, KUMA also performs a search by that resource. If the resource refers to other resources, KUMA also traverses these resources and searches in their content.

4. If you want to reset the search result, clear the **Search** field or click the × icon.

Viewing Kaspersky SIEM services

To view the services table:

1. In the web interface, open the **Resources** → **Active services** section.

2. If you want to update the table, click the **Update** button.

You can use the **Search** field to search for services by their names. Use regular expressions when searching for services.

You can sort the table by status, type, service name, version, tenant, fully qualified domain name, IP address, and API port by clicking the sort icon ⌄ in the column header and selecting **Ascending** or **Descending**.

The services table contains the following columns:

- **Status**—service status:

  - Green means the service is running and accessible from the KUMA Core server.

  - Red means that the service is not running or is not accessible from the KUMA Core server.

  - Yellow means that the service is running, but there are errors in the service log, or there are alerts for the service from Victoria Metrics. You can view the error message by hovering the mouse pointer over the service status. Yellow is the status that applies to all services except for the agent.

  - Purple means that the service configuration file has changed, but no other errors are present. If a service has an incorrect configuration file and has errors, for example, from Victoria Metrics, status of the service is yellow.

  - Gray means that an active service exists in the remote tenant and continues to run. Services with the gray status are kept when you delete the tenant to let you copy the ID and remove services on your servers. Only the General administrator can delete services with the gray status. When a tenant is deleted, the services of that tenant are assigned to the Main tenant.

- **Type**—type of service: **core, agent**, **collector**, **correlator**, **storage**, **event router**.

- **Name**—name of the service. Clicking on the name of the service opens its settings.
- **Version**—service version.
- **Tenant**—the name of the tenant that owns the service.
- **FQDN**—fully qualified domain name of the service server.
- **IP address**—IP address of the server where the service is installed.
- **API port**—Remote Procedure Call port number.
- **Uptime**—Uptime of the service.
- **Created**—the date and time when the service was created.
- **UUID**—Unique ID of the service.

If necessary, you can customize the columns by clicking the gear icon.

General instructions for working with services

This section provides general instructions for working with services.

Renaming a service

If necessary, you can change the name and settings of created services.

To rename the service:

1. In the web interface, open the **Resources** → **Active services** section.
2. Click the link with the name of the service in the **Service** column.
3. In the window that opens, specify a new service name and, if necessary, change the settings. The name must be unique within a tenant and contain 1 to 128 Unicode characters.

   For the KUMA Core and Metrics services, only the name can be changed.
4. Click the **Save** button.

Getting service identifier

When a service is created, each service is assigned an identifier, which is then used, for example, when installing the service on a server.

To get the identifier of a service:

1. In the web interface, open the **Resources** → **Active services** section.
2. In the context menu of the service whose ID you want to get, select **Copy ID**.

   The service identifier is copied to the clipboard.

Stopping, starting, and checking status of the service

To stop, start, or check the status of KUMA Core:

1. In the web interface, open **Resources** → **Active services**, and in the service context menu, select **Copy ID**.
   The ID will be copied to the clipboard.
2. On the command line, run one of the following commands:

   Stopping the service
   ```
   sudo systemctl stop kuma-core/collector/correlator/storage/metrics-<service_ID>.service
   ```

   Starting the service
   ```
   sudo systemctl start kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
   ```

   Checking the service status
   ```
   sudo systemctl status kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
   ```

   Where:
   <service_ID> is the service ID copied to the clipboard.

Stopping, starting, and checking the status of agents running on Windows

To stop or start an agent on Windows:

1. In the web interface, open the **Resources** → **Active services** section.
2. In the context menu of the agent whose ID you want to get, select **Copy ID**.
   The ID will be copied to the clipboard.
3. Connect to the host where you want to start or stop the KUMA agent.
4. Run PowerShell on behalf of an account with administrative rights.

5. In PowerShell, run one of the following commands:

```
Stopping the agent

Stop-Service -Name "WindowsAgent-<agent ID>"
```

```
Starting the agent

Start-Service -Name "WindowsAgent-<agent ID>"
```

To view the agent status:

1. On Windows, open the **Services** application.
2. In the list of services, double-click the KUMA agent whose status you want to view.
3. In the window that opens, view the status in the **Service status** field on the **General** tab.

Updating and restarting a service

To update or restart a service:

1. In the web interface, open the **Resources** → **Active services** section.
2. Select the check box next to the service and choose one of the following options:
   - If you want to update the settings of a running service without stopping it—for example, to change field mapping or destination settings—select **Update configuration**.
   - If you need to stop and restart the service—for example, to change the port or connector type—select **Restart**.

     Restarting KUMA agents:

     - The KUMA Windows agent can be restarted if it is running on a remote computer. If the service on the remote computer is inactive, an error when trying to restart it from KUMA will be displayed. In that case you must restart KUMA Windows Agent service on the remote Windows computer. For information on restarting Windows services, refer to the documentation specific to the operating system version of your remote Windows computer.
     - KUMA Agent for Linux stops when this option is used. To start the agent again, you must execute the command that was used to start it.

Deleting the service

To remove the service:

1. In the web interface, open the **Resources** → **Active services** section.
2. Get the identifier of the service to be removed. To do this, in the service context menu, click **Copy ID**.

3. In the context menu of the service, select **Delete**.

4. Confirm the removal.

5. Remove the service on the server by running the following command:

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage/eventRouter/metrics> --core https://<FQDN>:<port> --id <service_ID> --uninstall
```

Where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (7210 by default).
- <service_ID> is the service ID copied from the KUMA web interface.

```
For example:
```

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id 29fd6760-a870-42d2-8ebe-eb911ac90305 --uninstall
```

The service is uninstalled.

Versioning of resources and services

Kaspersky SIEM stores the history of changes to resources and services as versions. A version is created automatically when you create a resource or service, or change the settings of an existing one.

> The change history is not available for dictionaries. To save the history of dictionaries, you can export data.

Versions are retained for the duration specified in the **Settings** section. When the age of a version reaches the specified value, the version is automatically deleted.

You can view the change history of resources and services, compare versions, and restore a previous version, for example, when you need to recover the resource functionality.

Viewing the version

To view the change history of a resource or a service:

1. In the web interface, in the **Resources** section, select the required resource or service.

   If you want to view all resources and services, in the **Resources** section, go to the **List** tab.

2. Select the check box next to the resource or service whose change history you want to view.

3. In the toolbar or in the ⋮ menu, click **View versions history**.

   The version table opens.

You can sort the version table by the **Version**, **Published**, and **Author** columns by clicking the heading and selecting **Ascending** or **Descending**. You can also display in the table only changes made by specific users by clicking the heading of the **Author** column and selecting the authors as needed.

The resource table contains the following columns:

- **Version** is the serial number of the version. When you make changes to the resource or the service and create a new version, the serial number is increased by 1.

  The version with the highest number and the most recent publication date corresponds to the current state. Version 1 reflects the state of the resource or the service at the moment when it was created.

- **Published** is the date and time when the version was created.

- **Author** is the name of the user who saved the changes.

  If the changes were made by Kaspersky SIEM or by the migration script, the displayed value is **system**.

- **Comment** is a text comment added when saving changes, or a system comment describing the changes made.

- **Retention period** is the number of days and the date after which the version will be deleted.

  If necessary, you can configure the retention period for versions.

- **Actions** is the button that restores the version.

If you want to view the status of a resource or a service in a specific version, click that version in the table. In the pop-up window you can:

- View the settings of the selected version;

- Restore the version by clicking the **Restore** button;

- Export the version to a JSON file by clicking the **Export** button.

Comparing resource versions

You can compare any two versions, for example, if you need to track changes.

To compare versions:

1. In the web interface, in the **Resources** section, select the required resource or service.

   If you want to view all resources and services, in the **Resources** section, go to the **List** tab.

2. Select the check box next to the resource or service whose versions you want to compare.

3. In the toolbar or in the ⋮ menu, click **View versions history**.

   The version table opens.

4. Select the check boxes next to the versions you want to compare and click **Compare**.

A version comparison is displayed. Resource or service fields are displayed as a list or in JSON format. Differences between the two versions are highlighted. You can select other versions to compare using the drop-down lists.

Restoring a resource version

You can restore a previous version of a resource or a service, for example, if you need to recover the resource in case of mistakes made when making changes.

> Versions of automatically generated agents cannot be restored separately because they are created when the parent collector is modified. If you want to restore a version of an automatically generated agent, you need to restore the corresponding version of the parent collector.

To restore a previous version:

1. In the web interface, in the **Resources** section, select the required resource or service.

   If you want to view all resources and services, in the **Resources** section, go to the **List** tab.

2. Select the check box next to the resource or service whose version you want to restore.

3. In the toolbar or in the ⋮ menu, click **View versions history**.

   The version table opens.

4. In the row of the relevant version, in the **Action** column, click the **Restore** button.

   You can restore a version by clicking the row of this version, and then clicking the **Restore** button in the lower part of the window.

   > You can only restore previous versions. The **Restore** button is not available for the current version.

   > If the structure of a resource or service has changed after a Kaspersky SIEM update, restoring saved versions may be unavailable.

5. Confirm the action and, if necessary, add a comment. If you do not add a comment, the `Restored from v. <number of the restored version>` comment is automatically added to the version.

The version is restored as a new version and becomes the current version. If the resource for which you restored the version is added to the active service, this also changes the state of the service. You need to restart the service to apply the resource change.

Configuring the retention period for versions

> Only a user with the General administrator role can view and manage the retention period of versions.

To change the retention period of versions:

in the **Settings** → **Other** → **General** section, change the value of the **Resource history retention period, days** setting.

The default setting is 30 days. If you want to keep all versions without time limits, specify `0` (store indefinitely).

The retention period of versions is checked daily, and versions stored in Kaspersky SIEM for longer than the specified period are automatically deleted. In the **Task manager** section, the *Clearing resource change history* task is created to check the retention duration of versions and delete old ones. This task also runs after a restart of the KUMA Core.

You can check the time remaining until a version is deleted in the table of versions, in the **Retention period** column.

Viewing a dependency graph

For stable operation of the solution, it is important to understand how some resources and services affect the performance of others, what connections exist between resources and other KUMA objects. You can view these interdependencies on an interactive graph in the solution web interface.

Displaying dependencies on a graph

To view a dependency graph:

1. In the **Resources** section, select a resource or service.
2. Select the check box next to the resource or service whose links you want to view.
3. In the toolbar or menu (⋮), click the **Show dependencies** button.

   The dependency graph opens. To view the relevant part of the graph, use the graph map in the lower-right corner.

   Using the **Search** field, you can find the required node by its name, tag, path, or package.
4. If you want to download the dependency data, click the **Download SVG** button.
5. If necessary, configure filters to display dependencies on the graph using the **Show on graph** drop-down list.

Types of links in a graph

The graph displays all relations that are formed based on the universal unique identifier (UUID) of resources used in the configuration of the selected resource or service, as well as relations of resources that have the UUID of the selected resource in their configuration. Links referenced (used) by the selected resource or service are displayed up to the last level. For links that reference the selected resource or a service, only one level is displayed.

Types of links:

- Solid line without a caption.

  Represents a direct link by UUID, including the use of secrets and proxy servers in integrations.

- Line captioned **<function_name>**.

Represents the use of an active list in a correlation rule.

- Dotted line captioned **linked**.

  Represents a link by URL, for example, of a destination with a collector, or of a destination with a storage.

Resources displayed on the graph

On the graph, you can view the relations of the following resources:

Correlation rules

Aggregation rules

Enrichment rules

Response rules

Data mining rules

Normalizers

Connectors

Destinations

Filters

Dashboards

Dashboards are not part of other resources; therefore, there are no links to resources that reference dashboards.

Report templates

Report templates are not part of other resources, therefore there are no links with resources that reference report templates.

Notification templates

Active lists

Dictionaries

Proxy servers

Secrets

Context tables

Collectors

If a collector was initially selected to display links, links to resources that refer to this collector are not displayed.

Correlators

Storages

Agents (autoagents)

If an agent is selected for displaying links, the collector is displayed with the **linked** relation type only if the collector is running as a service and is correctly (FQDN and port) specified in the agent destination settings.

Event routers

If an event router was initially selected to display links, the links to resources that refer to this event router are not displayed.

Integrations

The name of the integration corresponds to the name of the tab in the **Integrations** section.

Inaccessible resource (if you do not have the rights to view it).

When you click a resource node, the following information about the resource is displayed: **Name**, **Type**, **Path**, **Tags**, **Tenant**, and **Package name**. When you click the name, information about the resource or service opens in a separate tab.

Configuring the display of nodes and links in the graph

The display of nodes and relationships in the graph is performed via the node context menu, which provides the following actions:

- **Show resource dependencies**.

  The dependencies of the resource or service are displayed.

- **Hide resource**.

  The resource is hidden. Linked resources or services are marked with a link icon ( ). The links in the graph will be broken.

- **Hide resources of this type**.

  All resources of the selected type will be hidden.

- **Hide resource relations**.

  The resource or service will be marked with a link icon ( ) indicating that it has hidden links.

- **Update resource relations**.

  Visible links that have changed while working with the graph will be updated.

- **Group**.

  The action is available if there are more than 10 links of the same type to a resource.

Tag management

For the convenience of working with resources, tags are provided. Using the tags, you can quickly find the relevant resource.

Tags can be added only in the resource settings. You cannot add tags to resources that are created from the interface of other resources. You also cannot add tags to a resource that is not editable.

Viewing tags

To view tags,

in the web interface, open the **Settings** → **Other** → **Tags** section.

The tags table opens.

You can use the **Search** field to search for tags by their names. Regular expressions are used when searching for tags.

You can sort the table by name and usage quantity in resources by clicking the sort icon in the column header and selecting **Ascending** or **Descending**.

The tags table contains the following columns:

- **Name** is a tag name.

- **Tenant** is the tag to which the tag belongs. To search for tags, click the sort icon in the column header, and specify a value to search for in the **Search** field or select types using check boxes.

- **Used in resources** shows information on how many resources have been tagged. Clicking the number takes you to the list of resources for the selected tag.

Adding a tag

To add a tag:

1. In the **Resources** section, click the service or resource for which you want to add a tag.
2. Select a service or resource in one of the following ways:
   - Click the service or resource name.
   - Select the check box next to the service or resource and, in the toolbar or menu ⋮, click **Tags** → **Link**.
3. In the panel that opens, enter a tag or select a tag from the drop-down list.

   You can add multiple tags.

   The tag name can contain uppercase and lowercase letters, numbers, underscores, and spaces. Once added, the tag is always displayed in lowercase.
4. Click **Save**.

The tag is added.

Removing a tag

To remove a tag:

1. In the **Resources** section, click the service or resource for which you want to add a tag.
2. Select a service or resource in one of the following ways:
   - Click the service or resource name.
   - Select the check box next to the service or resource and, in the toolbar or menu ⋮, click **Tags** → **Unlink**.
3. In the panel that opens, click the X icon next to the tags that you want to remove.
4. Click **Save**.

The tag is removed.

Folder management

Resources can be organized into folders. The folder structure is displayed in the left part of the window. Root folders correspond to tenants and contain a list of all resources of the tenant. Resources in this folder are displayed in subfolders. When a folder is selected, the resources it contains are displayed as a table in the right pane of the window.

You can create, rename, add to favorites, move, and delete folders. You can also move resources between folders.

Creating a folder

To create a folder:

1. In the **Resources** section, select a resource or service.
2. In the tree, select the tenant folder in which you want to create a subfolder.
3. Click the plus icon (+).
4. This opens a window; in that window, enter the folder name and click **Add**.

   The folder will be created.

Changing a folder

To rename a folder:

1. In the **Resources** section, select the resource or service whose folder you want to rename.
2. In a tree, hover over the folder name.
3. In the menu ⋮ on the right, select **Rename**.
4. Enter a new folder name, and save changes.

   The folder will be renamed.

Adding a folder to favorites

To add a folder to favorites:

1. In the **Resources** section, select a resource or service.
2. In the tree, hover over the folder that you want to add to favorites.
3. In the menu ⋮ on the right, select **Add to favorites**.
   The folder is added to favorites.
4. If you want to remove a folder from favorites, in the menu ⋮ on the right, select **Remove from favorites**.

   The folder is added to favorites.

Moving the folder

> Folders cannot be moved from one tenant to another.

To move a folder:

1. In the **Resources** section, select a resource or service.
2. In a tree, click the folder name, and drag it to the required location in the folder structure.

   The folder will be moved.

Moving resources or services

> You can only move resources to folders of the tenant for which the resources were created. Resources cannot be moved to folders in another tenant.

To move a resource or service to another folder:

1. In the **Resources** section, select a resource or service.
2. Select the check boxes next to the resources or services that you want to move.

   The number of selected resources is displayed in the lower part of the table.
3. Use the ⣿ icon to drag and drop resources into the required folder.

   Resources or services are moved.

Deleting a folder

You can delete a folder even if it contains subfolders, resources, or services. Before deleting, you need to confirm the action by entering a generated value. If there are dependent resources in the folder, a list of dependencies is displayed in the confirmation window.

To delete a folder:

1. In the **Resources** section, select a resource or service.
2. In the tree, point to the folder name that you want to delete.
3. In the menu ⋮ on the right, select **Delete**.

4. Enter the generated value.

5. Confirm the deletion.

The folder will be deleted.

Analyzing data and working with security incidents

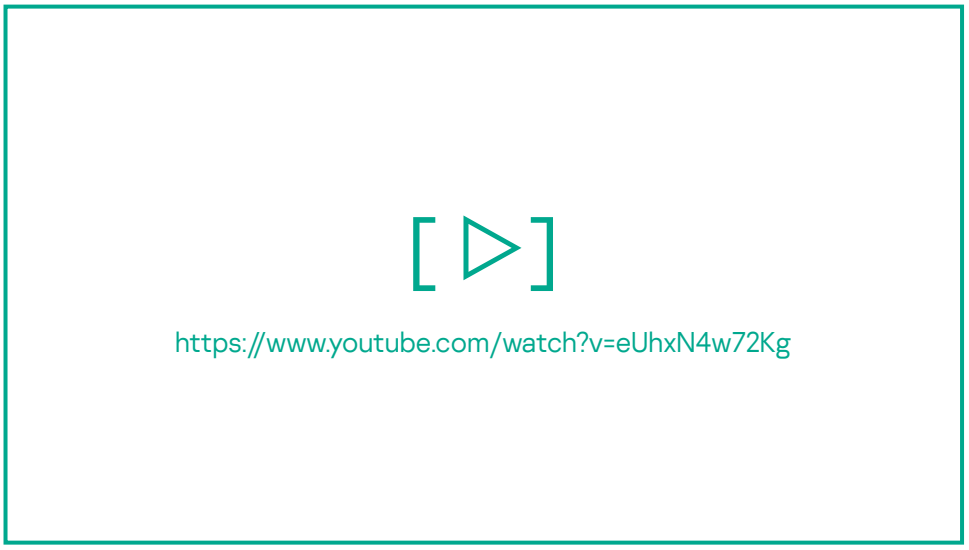
This section provides instructions for analyzing data and working with security incidents in Kaspersky SIEM.

Security monitoring

The Kaspersky SIEM solution provides the following tools for monitoring the security of your organization's network:

- dashboards, which are a set of widgets;
- reports;
- notifications.

To learn more about working with dashboards and reports, watch this video:



Dashboards

In the **Dashboards** section, you can monitor the security status of your organization's network.

The dashboard is a set of widgets that display network security data analytics. Data viewing is available only for tenants to which you have access.

To learn more about the dashboards, watch this video:

https://www.youtube.com/watch?v=eUhxN4w72Kg

You can create dashboards manually or use predefined dashboards. If necessary, you can manage the settings of the widgets in the predefined dashboards. The predefined **Alerts Overview** dashboard is used as the default dashboard.

Only users with General Administrator, Tenant administrator, Tier 2 analyst, and Tier 1 analyst roles can create, manage, or delete dashboards. Users with accounts of all roles can view dashboards and set default dashboards. If a dashboard is set as default, that dashboard is displayed for the account every time the user navigates to the **Dashboards** section. The selected default dashboard is saved for the current user account.

The information in the **Dashboards** section is updated in accordance with the schedule configured in dashboards settings. If necessary, you can force the update of the data.

For convenient presentation of information on dashboards, you can enable TV mode. This mode lets you view the dashboards in full-screen mode in FullHD resolution. In TV mode, you can also configure a slide show display for the selected dashboards.

If necessary, you can view a list of all available dashboards for tenants to which they belong in the left part of the window. You can click the **Hide dashboards** button to collapse this list, in which case the widgets of existing dashboards are displayed. You can bring back the list of all dashboards available for tenants by clicking the **Show dashboards** button.

In the list of all dashboards available for tenants, you can also click the add icon + to create folders for grouping dashboards in tenants. You can manage the settings of these folders or delete them by clicking the menu icon ⋮ and selecting an action.

Predefined dashboards

KUMA comes with a set of predefined dashboards: The default refresh period for predefined dashboards is **Never**. You can modify these dashboards as necessary.

Dashboards such as [OOTB] KSMG files and hashes, [OOTB] KSMG rules and URLs, [OOTB] KSMG results, and [OOTB] KSMG email subjects and accounts have been available since KUMA 3.4.1. Widgets will correctly display information when using the "[OOTB] KSMG 2.1+ syslog CEF" normalizer.

The table below describes the predefined dashboards and the widgets included in these dashboards.

Dashboard name	Description of widgets in the dashboards
Alerts Overview	• Active alerts—number of alerts that have not been closed. • Unassigned alerts—number of alerts that have the **New** status. • Latest alerts—table with information about the last 10 unclosed alerts belonging to the tenants selected in the dashboard. • Alerts distribution—number of alerts created during the period configured for the widget. • Alerts by severity—number of unclosed alerts grouped by their severity. • Alerts by assignee—number of alerts with the **Assigned** status. The grouping is by account name. • Alerts by status—number of alerts that have the **New**, **Opened**, **Assigned**, or **Escalated** status. The grouping is by status. • Affected users in alerts—number of users associated with alerts that have the **New**, **Assigned**, or **Escalated** status. The grouping is by account name. • Affected assets—table with information about the level of importance of assets and the number of unclosed alerts they are associated with. • Affected assets categories—categories of assets associated with unclosed alerts. • Top event source by alerts number—number of alerts with the **New**, **Assigned**, or **Escalated** status, grouped by alert source (DeviceProduct event field). The widget displays up to 10 event sources. • Alerts by rule—number of alerts with the **New**, **Assigned**, or **Escalated** status, grouped by correlation rules.
Incidents Overview	• Active incidents—number of incidents that have not been closed. • Unassigned incidents—number of incidents that have the **Opened** status. • Latest incidents—table with information about the last 10 unclosed incidents belonging to the tenants selected in the dashboard. • Incidents distribution—number of incidents created during the period configured for the widget. • Incidents by severity—number of unclosed incidents grouped by their severity. • Incidents by assignee—number of incidents with the **Assigned** status. The grouping is by user account name. • Incidents by status—number of incidents grouped by their status. • Affected assets in incidents—number of assets associated with unclosed incidents. • Affected users in incidents—users associated with unclosed incidents. • Affected asset categories in incidents—categories of assets associated with unclosed incidents. • Active incidents by tenant—number of incidents of all statuses, grouped by tenant.
Network Overview	• Netflow top internal IPs—total volume of netflow traffic received by the asset, in bytes. The data is grouped by internal IP addresses of assets. The widget displays up to 10 IP addresses. • Netflow top external IPs—total volume of netflow traffic received by the asset, in bytes. The data is grouped by external IP addresses of assets. • Netflow top hosts for remote control—number of events associated with access attempts to one of the following ports: 3389, 22, 135. The data is grouped by asset name. • Netflow total bytes by internal ports—number of bytes sent to internal ports of assets. The data is grouped by port number. • Top Log Sources by Events count—top 10 sources from which the greatest number of events was received.
[OOTB] KATA & EDR	• KATA. Top-10 detections by type—visualizes the 10 most common types of events detected by the KATA system. • KATA. Top-10 detections by file type—visualizes the 10 most common file types detected by the KATA system. • KATA. Top-10 user names in detections—visualizes the 10 most common user names detected by the KATA system. • KATA. Top-10 IDS detections—visualizes the 10 most common threats detected by the IDS module of the KATA system. • KATA. Top-10 URL detections—visualizes the 10 most common suspicious URLs detected by the KATA system. • KATA. Top-10 AV detections—visualizes the 10 most common threats detected by the KATA anti-virus module. • EDR. Top-10 MITRE technique detections—visualizes the 10 most common MITRE ATT&CK matrix techniques detected by the EDR system. • EDR. Top-10 MITRE tactic detections—visualizes the 10 most common MITRE ATT&CK matrix tactics detected by the EDR system.
[OOTB] KSC	• KSC. Top-10 users with the most KAV alerts—visualizes the 10 most common user names present in events related to the detection of malicious software, information about which is contained in the KSC system. • KSC. Top-10 most common threats—visualizes the 10 most common types of malware, information about which is contained in the KSC system. • KSC. Number of devices that received AV database updates—visualizes the number of devices on which anti-virus database updates have been installed, information about which is contained in the KSC system. • KSC. Number of devices on which the virus was found—visualizes the number of devices on which malware was detected, information about which is contained in the KSC system. • KSC. Malware detections by hour—visualizes the distribution of the number of malware per hour, information about which is contained in the KSC system.
[OOTB] KSMG	• KSMG. Top-10 senders of blocked emails—visualizes the 10 most common senders of email messages blocked by the KSMG system. • KSMG. Top-10 events by action—visualizes the 10 most common actions performed by the KSMG system. • KSMG. Top-10 events by outcome—visualizes the 10 most common results of actions performed by the KSMG system. • KSMG. Blocked emails by hour—visualizes the distribution of the number of email messages blocked by the KSMG system, by hour.

Dashboard name	Description of widgets in the dashboards
[OOTB] KWTS	• KWTS. Top-10 IP addresses with the most blocked web traffic—visualizes the 10 most common IP addresses from which traffic blocked by the KWTS system originated. • KWTS. Top-10 IP addresses with the most allowed web traffic—visualizes the 10 most common IP addresses from which traffic allowed by the KWTS system originated. • KWTS. Top 10 requests by client application—visualizes the 10 most common applications used to gain access to network resources, as detected by the KWTS system. • KWTS. Top-10 blocked URLs—visualizes the 10 most common URLs from which traffic was allowed by the KWTS system. • KWTS. System action types—visualizes the 10 most common actions performed by the KWTS system. • KWTS. Top-10 users with the most allowed web traffic—visualizes the 10 most common user names of users whose traffic was allowed by the KWTS system.
[OOTB] KSMG files and hashes	• KSMG. Top-5 blocked hashes—visualizes five most common file hashes in email messages blocked by the KSMG system. • KSMG. Top-5 net-transferred hashes—visualizes five most common "clean" file hashes in email messages tracked by the KSMG system. • KSMG. Top-5 clean file names—visualizes five most common "clean" file names in email messages tracked by the KSMG system. • KSMG. Top-5 blocked files—visualizes five most common file names in email messages blocked by the KSMG system.
[OOTB] KSMG rules and URLs	• KSMG. Top-5 rules—visualizes the 5 most common triggered rules of the KSMG system. • KSMG. Top-5 URLs—visualizes five most common domains from links in email messages tracked by the KSMG system.
[OOTB] KSMG results	• KSMG. All results in the last 24 hours—visualizes the hour-by-hour distribution of actions performed by the KSMG system during the last 24-hour period. • KSMG. Top-5 results—visualizes five most common actions performed by the KSMG system.
[OOTB] KSMG email subjects and accounts	• KSMG. Top-5 email subjects—visualizes five most common subjects of email messages tracked by the KSMG system. • KSMG. Top-5 source accounts—visualizes five most common sender accounts of email messages tracked by the KSMG system. • KSMG. Top-5 destination accounts—visualizes five most common recipient accounts of email messages tracked by the KSMG system.

Availability of dashboards in different tenants

The properties of dashboards created in the Shared tenant differ from those of dashboards created in other tenants.

Dashboards in the Shared tenant

If dashboard is created in the Shared tenant, it has the following properties:

- The universal dashboard can be viewed by all user roles and in all tenants.
- Data for tenants is displayed in accordance with the general tenant filter.
- Data in widgets on events from the database is obtained in accordance with the space settings configured for the user.

To manage the dashboard in the Shared tenant, the user needs to have the following roles:

- Manage shared resources: for creating resources, changing settings, and deleting resources. Users with this role get access to all shared resources.
- Read shared resources: viewing a list of universal dashboards. With this role, the user gets read access to all shared resources in the **Resources** section.

If you have a role that grants access to dashboards in the Shared tenant, you can view the list of universal dashboards in the **Dashboards** and **Resources** sections, but you do not have access to other resources of the Shared tenant.

To view the current data of dashboards in the Shared tenant, subscribe to changes in such dashboards. You can subscribe to all dashboards, including those created by you, in the Shared tenant.

To subscribe to a dashboard in the Shared tenant:

1. In the **Dashboards** section, in the list of dashboards, select and open a dashboard in the Shared tenant.
2. Click the menu ⋮ icon in the upper right corner of the open dashboard.
3. In the menu, select **Subscribe on changes**.

   If necessary, you can unsubscribe by selecting **Unsubscribe from changes** in the list of actions.

If a user's role involves managing CII resources, the display of information on the dashboard takes into account the CII attribute.

Dashboards in other tenants

Dashboards created in any KUMA tenant, except for the Shared tenant, have the following properties:

- The dashboards can be viewed by users that have access to the tenant in which the dashboard was created.
- Only users that have access to the tenant in which the dashboard was created have access to the data of the widgets in the dashboard.
- If the dashboard has the CII attribute, the data on the dashboard is available to users whose rights allow access to CII.

Dashboard management

This article describes how to create, edit, and remove dashboards.

Creating a dashboard

To create a dashboard:

1. In the web interface, open the **Dashboards** section.

   You can also create a dashboard in the **Resources** section of the **List** tab. To do this, click the **Add** button and select the **Dashboard** resource type.
2. Do one of the following:
   - In the toolbar or in the menu (⋮), click **Create dashboard**.
   - Click the **Create dashboard** button under the list of all dashboards.

This opens the dashboard settings window.

3. In that window, specify a unique name for the dashboard. The name must contain from 1 to 128 Unicode characters and must be unique within the selected tenant.

   A custom dashboard cannot have the same name as a predefined dashboard.

   An error is returned when trying to create a dashboard with the same name as a predefined dashboard or change the name of a custom dashboard to the name of a predefined dashboard in the Main tenant. In tenants other than Main, you can create or duplicate a custom dashboard with the same name as a predefined dashboard.

4. In the **Dashboard tenant** drop-down list, select the tenant that will own the new dashboard, or a certain folder in the tenant.

   If you had any set of charts from a folder in the tenant open before creating the dashboard, KUMA automatically specifies this tenant when creating the dashboard. You can change the tenant as necessary.

5. In the **Collect data from tenants** drop-down list, select one or more tenants whose data you want to be represented in the dashboard.

6. If necessary, in the **Time period** drop-down list, select the time period from which you want to get analytics in one of the following ways:

   - If you want to specify an **exact date**, select start and end dates of the period in the calendar and click **Apply**.

     You can select a date up to and including the current date. The date and time format depends on your browser settings. If the **Range from** or **Range to** field has a value and you have not edited the time value manually, when you select a date in the calendar, the **Range from** field is automatically populated with `00:00:00,000`, and the **Date to** field is populated with `23:59:59,999`. If you have manually deleted the value in the **Range from** or **Range to** field, when you select a date in the calendar, the field is automatically populated with the current time. Once you select a value in one of the fields, the focus switches to the other field. If your **Range to** is earlier than your **Range from**, this earlier value is automatically inserted into the **Range from** field.

   - If you want to specify a **relative period**, select one of the periods available in the **Relative period** list.

     The period is calculated relative to the current time.

   - If you want to specify a **custom period**, set or edit the value of the **Range from** and **Range to** fields manually.

     You can enter an exact date and time in the `DD.MM.YYYY HH:mm:ss.SSS` format for the Russian localization and `YYYY-MM-DD HH:mm:ss.SSS` for the English localization or a period relative to the current time as a formula. You can also combine these methods. If you do not specify milliseconds when entering the exact date, `000` is substituted automatically. If you have edited the time in the **Range from** or **Range to** fields, picking a date in the calendar does not change the time component.

     In the relative period formulas, you can use the `now` parameter for the current date and time and the interval parameterization language: `+` (only in the **Range to** field), `-`, `/` (rounding to the nearest), as well as time units: `y` (year), `M` (month), `w` (week), `d` (day), `h` (hour), `m` (minute), `s` (second). For example, you can specify the period `now-5d` to get data for the last five days, or `now/w` to get data from the beginning of the first day of the current week (00:00:00:000 UTC) to the current time (`now`).

     > The **Range from** field is required, and its value cannot exceed the value of the **Range to** field, and also cannot be earlier than 1970-01-01 (if specifying an exact date or a relative period). The **Range to** cannot be earlier than the **Range from**. If you do not specify a value in the **Range to** from field, `now` is specified automatically.

By default, the **1 day** (**now-1d**) relative period is selected. The bounds of the period are inclusive: for example, for the **Today** time range, events are displayed from the beginning (00:00:00:000 UTC) of the current day to the current time (**now**) inclusive, and for the **Yesterday** period, events are displayed from the beginning (00:00:00:000 UTC) of the previous day to 00:00:00:000 UTC of the current day.

Kaspersky SIEM stores time values in UTC, but in the web interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the data display period, data will be displayed for the period from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative data display period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the **Range from** and **Range to** (if a value other than `now` is specified) by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want to display data for **Yesterday**, you need to change **Range from** to `now-1d/d-3h` and **Date to** to `now/d-3h`. If you want to display data for the **Today** period, you only need to change the value in the **Range from** field to `now/d-3h`.

> If you need results up to 23:59:59:999 UTC of yesterday, you can use an SQL query with a filter by Timestamp or specify an exact date and time.

7. If necessary, in the **Refresh interval** drop-down list, select the data refresh period in the dashboard widgets:
   - **No refresh** means data in dashboard widgets are never refreshed.
   - **1 minute**
   - **5 minutes**
   - **15 minutes**
   - **1 hour** (default)
   - **3 hours**
   - **6 hours**
   - **12 hours**
   - **24 hours**
8. If necessary, select tags for the dashboard from the **Tags** drop-down list.
9. If necessary, add a description of the dashboard.
10. Use the **CII status** toggle switch to enable the display of information for assets, alerts, and incidents related to critical information infrastructure (CII). This makes such dashboards viewable only by users whose settings have the **Access to CII facilities** check box selected.

    If this toggle switch is disabled, widgets of the dashboard do not display information for assets, alerts, and incidents related to critical information infrastructure (CII) even if the user has access to CII facilities.
11. Click **Apply**.
12. Click the **Add widget** button and select a widget. This opens a window; in that window, configure the selected widget.

You can add multiple widgets. You can drag widgets around the window by the handle icon (⠿) in the upper left corner of the widget. If you need to resize the widget, you can do so using the arrow icon (⤡) that is displayed when you hover over the lower right corner of the widget.

The following limitations apply to widgets with the **Pie chart**, **Bar chart**, **Line chart**, **Counter** , and **Date Histogram** chart types:

- In `SELECT` queries, you can use extended event schema fields of `String`, `Number`, and `Float` types.
- In `WHERE` queries, you can use all types of extended event schema fields (`String`, `Number`, `Float`, `Array of strings`, `Array of numbers`, and `Array of floats`).

For widgets with the **Table** chart type, in `SELECT` queries, you can use all types of extended event schema fields (`String`, `Number`, `Float`, `Array of strings`, `Array of numbers`, and `Array of floats`).

By clicking the menu (⋮) icon in the upper right corner of the widget, you can do the following:

- Manage the settings of widgets
- Create copies of widgets
- Remove widgets
- Download widget data in CSV format

13. Click **Create**.

The new dashboard is created and displayed in the **Dashboards** section of the KUMA web interface.

Changing the dashboard

To manage dashboard settings:

1. In the web interface, open the **Dashboards** section.
2. Expand the list of folders with dashboards in the upper left corner of the **Dashboards** window.
3. Click the relevant dashboard.
4. Click the menu icon ⋮ next to the dashboard in the list of folders with dashboards, and in the menu, select **Edit**.
5. Make your changes in the window that is displayed. The settings that are available for editing are the same as the settings available when creating a dashboard.
6. Click the **Save** button.

The dashboard settings are modified.

If the dashboard was removed or assigned to a different tenant while you were managing its settings, an error is displayed when you click the **Save** button. The dashboard is not saved. Refresh the KUMA web interface page to see the list of available dashboards in the drop-down list.

Removing a dashboard

To remove a dashboard:

1. In the web interface, open the **Dashboards** section.

2. If necessary, click the **Show dashboards** button in the upper left corner of the **Dashboards** window and open the list of folders with dashboards.

3. Click the relevant dashboard.

4. Do one of the following:

   - Click the menu icon ⋮ next to the dashboard in the list of folders with dashboards, and in the menu, select **Remove**.

   - Click the menu icon ⋮ in the upper right corner of the **Dashboards** window with the dashboard open, and in the menu, select **Remove**.

5. Confirm the removal.

The dashboard is removed.

Selecting a dashboard

To view a dashboard or select a default dashboard:

1. Expand the list of folders with dashboards in the upper left corner of the **Dashboards** window.

   Folders with dashboards are organized in accordance with the tenants they belong to.

2. If you want to view the dashboards that you have created, click the **Created by me** button.

   KUMA displays only the dashboards that you have created and only those folders where these dashboards are located. The folders in which your dashboards are located may have been created by other users.

3. Select a folder and a dashboard in that folder.

   The selected dashboard is displayed in the **Dashboards** window of the KUMA web interface.

4. You can set the selected dashboard as the default dashboard. To do so, follow one of these steps:

   - Click the menu icon ⋮ next to the dashboard in the list of folders with dashboards, and select **Use by default**.

   - Click the menu icon ⋮ in the upper right corner of the **Dashboards** window with the dashboard open, and select **Set as default**.

   The selected dashboard is marked with the **Default** attribute and becomes the default dashboard.

Enabling and disabling the TV mode

Once the TV mode is enabled, you will be navigated to the full-screen dashboards view mode in FullHD resolution.

> To display analytics in TV mode, we recommend creating a separate user with the minimum required set of rights.
> If changes are made to the dashboards selected for the slideshow, those changes are automatically reflected in the running slideshow sessions.

To enable TV mode:

1. In the KUMA web interface, select the **Dashboards** section.
2. Click the **TV mode** button in the upper right corner.
3. In the displayed window, move the **TV mode** toggle switch to the **Enabled** position.
4. To configure the dashboard slideshow:
   a. Move the **Slideshow** toggle switch to the **Enabled** position.
   b. In the **Timeout** field, specify how long each dashboard is displayed, in seconds.
   c. Under **Queue**, select the dashboards to display and click **Add to queue**. If no dashboard is selected, the slideshow iterates through all dashboards available to the user.
   d. If necessary, you can delete a dashboard. To do this, select the check box of the dashboard in the queue and click **Delete**.
   e. If necessary, you can change the order of the dashboards by dragging them with the right mouse button.
5. Click the **Save** button.

   TV mode will be enabled.

To disable TV mode:

Click the **Stop** button in the upper right corner of the window where the dashboards are displayed.

TV mode is disabled. The left part of the screen shows a pane containing sections of the KUMA web interface.

Selecting the period without modifying dashboard settings

When viewing the KUMA dashboard, the period that is specified in the dashboard settings is displayed. If you need to view data for a different period, you can set a period without changing the dashboard settings.

To change the period in the dashboard:

1. In the **Dashboards** section of the KUMA web interface, select a dashboard to display.

   The selected dashboard is displayed in the **Dashboards** window. When opened, the dashboard is generated in accordance with the last scheduled data update.

2. In the **Period** drop-down list above the dashboard, select the absolute or relative period that you are interested in.

3. If you have selected an absolute period, click the **Apply** button.

   The dashboard data is updated.

When changing the period in the dashboard, consider the following:

- The period that you set as described above is not saved in the settings of the dashboard. If you refresh the browser page or close and reopen the dashboard, the display period reverts to the one specified in the dashboard settings.

- Widgets on the dashboard respect the set period. If you specify a different period in the dashboard, the data only changes in widgets for which the **Period** value **as in the dashboard** .

- In TV mode, data is not interactive, therefore the **Period** drop-down list is not displayed and setting a new period is not possible.

Exporting dashboards

Consider the following when exporting dashboards:

- Dashboards are exported without tenants, storage, and space information because these parameters are configured individually for each KUMA instance.

- Dashboard widgets are exported without tenant, storage, and space information.

- The parameters of the enrich and lookup SQL functions in widget queries are exported unchanged. If necessary, you can modify these in accordance with your requirements after exporting resources.

- Links to active lists and tables are not exported. If necessary, you can customize these widgets after exporting resources.

To export a dashboard:

1. In the **Resources** section, go to the **List** tab.

   This opens a window with a list of all resources available to you in KUMA.

   If necessary, you can configure the display of resources in the list by selecting **Dashboard** in the **Resource kind** column.

2. Select the check box next to the dashboard that you want to export.

3. Click the **Export** button above the table of resources.

4. In the sidebar that is displayed:

   a. Enter the password for the file with exported resources. The password must satisfy the following requirements:

      - At least 16 characters.
      - At least one lowercase character.
      - At least one uppercase character.
      - At lease one numeral.
      - At least one special character.

   b. In the **Tenant** drop-down list, select the tenant from which you want to export the selected resources.

   c. Check boxes near the resources you want to export.

      If you select the **All resources** check box, all resources in folders of the selected tenant are exported.

5. Click the **Export** button.

The exported file will be saved to the downloads folder of your browser.

Importing dashboards

Consider the following when importing dashboards:

- If you import a dashboard into the selected tenant and the `exportID` of the imported dashboard is the same as the `exportID` of a dashboard that is already present in the tenant, a conflict message is returned with suggestions on how to resolve the conflict:

  - **Skip**

    If you select **Skip**, all resources selected for import are imported, except the conflicting resource.

  - **Replace**.

    If you select **Replace**, the dashboard is imported and the data is overwritten.

  If you want to look at the difference between dashboards with the same exportID, you can click **Skip**, and then import the dashboard into another tenant and compare the dashboards in different tenants.

- If the name of the imported dashboard is the same as the name of the dashboard that is already present in the tenant, the dashboard is imported and the date and time of the import is appended to the name. For example, Alerts Overview-2025-11-26 12:52:59.

- If the dashboard contains an **Events** widget, we recommend importing the dashboard into the **Shared** tenant. This makes the dashboard universal.

- Importing a dashboard into the Shared tenant requires the **Manage shared resources** role. To view such a dashboard, you need to subscribe to the dashboard.

- If the dashboard is imported into the **Shared** tenant, all storages are automatically specified in the dashboard because access to these is governed by user settings.

- If a dashboard is imported into any tenant other than **Shared**, the tenant of the imported dashboard is specified as the resource tenant, the data source tenant, and the storage tenant. After importing resources, you need to specify spaces for widgets with events and if necessary, expand the list of tenants.

- The parameters of the enrich and lookup SQL functions in widget queries are imported unchanged. If necessary, you can modify these in accordance with your requirements after importing resources.

- Links to active lists and tables are not imported. If necessary, you can customize these widgets after importing resources.

- If the dashboard contains the **Active lists** or the **Context tables** widget, we recommend duplicating such dashboards and editing the settings of the duplicates to adapt them to your infrastructure: specifying a correlator, selecting active lists and context tables.

To import a dashboard:

1. In the **Resources** section, go to the **List** tab.

   This opens a window with a list of all resources available to you in KUMA.

   If necessary, you can configure the display of resources in the list by selecting **Dashboard** in the **Resource kind** column.

2. Use the check box to select the dashboard to be imported.

3. Click the **Import** button above the table of resources.

4. In the sidebar, in the **Tenant** drop-down list, select the tenant to which you want to import the dashboard.

5. Select the import source: **File** or **Repository**.

6. Depending on the selected import source, follow these steps:

   a. If you selected **File** as the import source, follow these steps:

      - Specify the password for the imported file.

      - Click the **Select file** button to select the file that you want to import.

      - Select the check boxes of the resources that you want to import.

   b. If you selected **Repository** as the import source, select one or more repository packages in the displayed table.

7. Click the **Import** button.

8. If necessary, resolve conflicts between the resources imported from the file and the existing resources.

Reports

In Kaspersky SIEM, you can configure the regular generation of reports on the status of processes and objects in your organization's network.

Reports are generated based on *report templates*.

Reports can be generated manually, or you can configure a schedule for automatic report generation.

> When deploying KUMA in a high availability configuration, the time zone of the KUMA Core server and the time in a user's browser may differ. This difference is manifested by the discrepancy between the time in reports generated by schedule and the data that the user can export from widgets. To avoid this discrepancy, configure the report generation schedule to take into account the difference between the user and UTC time zones.

To learn more about working with reports, watch this video:

https://www.youtube.com/watch?v=3uapwg0Pq04

Availability of report templates across different tenants

In order for a report template to be available to users of all tenants, it must be created in the Shared tenant. Report templates created in other tenants are available only to users of these tenants (if users are not assigned the General Administrator role).

To work with a report template created in the Shared tenant, the user must have these roles:

- For creation, management, or deletion, the Manage shared resources role is needed. This role rights grant access to all shared resources.

  The CII attribute can be set by any user with the Manage shared resources role if the user's role involves managing CII resources.

- The Read shared resources role allows viewing the list of universal report templates. This role grants a user read access to all shared resources.

Widgets in a report template created in the Shared tenant are displayed according to these rules:

- Widget data for tenants is displayed according to the user's access to tenants, the global tenant filter, and the configuration of the report template or widget.

- You can view the widget data when managing report template settings by clicking the **Update preview** button.

- Event widget data is received from the database in accordance with the space set settings of the user. If, when generating a report, it turns out that the user does not have access to the spaces of one or more tenants, KUMA generates an empty report and displays a message indicating that other results cannot be provided because of the lack of access to the relevant spaces.

- Widget data in the report can include or exclude CII. For access to reports in which data includes CII, the user must have the Interaction with CII role.
- Limitations for active list and context table widgets apply to universal reports.

Viewing generated reports

To view reports:

1. In the web interface, go to the **Reports** section and do one of the following:
   - To view all generated reports, select **Generated reports**.
   - To view reports for a specific template, select the check box next to the template name and, in the toolbar or menu ⋮, click **View all generated reports**.

   The table of generated reports appears.

   You can search for reports by names using the **Search** field.

   You can sort the table by name and creation time by clicking the sort icon ⌄ in the column header and selecting **Ascending** or **Descending**.
2. If you want to view a specific report, click that report.

   A report window with configured widgets opens. If a widget displays information about events, alerts, incidents, active lists, or context tables, you can click its header to open the corresponding section of the web interface with an active filter and/or search query that is used to display data from the widget. Default values are applied to widgets.

The report table contains the following columns:

- **Name**—the name of a report.
- **Time period**—the time period for which report analytics was received.
- **Last report**—the date and time when a report was generated.
- **Tenant**—name of the tenant that owns the report.
- **User**—name of the user who generated the report manually. If the report was generated by schedule, the value is blank.

If necessary, you can customize the columns by clicking the gear ⚙ icon.

Viewing report templates

Reports are generated from templates. The template specifies the request, data display parameters, and the schedule for report generation.

> Users with the following roles can create, edit, and delete report templates: General Administrator, Tenant Administrator, Level 2 Analyst, and Level 1 Analyst.

To view report templates,

in the web interface, go to the **Reports** section and select the **Templates** tab.

The table of report templates opens.

You can use the **Search** field to search for report templates by their names. Regular expressions are used when searching for report templates.

You can sort the table by name, last update time, or package name by clicking the sort icon ⌄ in the column header and selecting either **Ascending** or **Descending**.

The template table contains the following columns:

- **Name** is the name of the report template.
- **Tenant** is the name of the tenant that owns the report template.
- **Updated** is the date and time of the last update of a resource template.
- **Created by** is the name of the user who created the report template.
- **Description** is optional information about the report template.
- **Tags** to help find the report template. You can search for report templates by clicking the sort icon ⌄ in the column header, by specifying a value to search for in the **Search** field, or by selecting tags using check boxes.
- **Schedule** is the rate at which reports must be generated using the template. If the report schedule was not configured, the **disabled** value is displayed.
- **Send by email** indicates that email notification is configured for generated reports.
- **Last report** is the date and time when the last report was generated based on the report template.
- **Package name** is the name of the package of tools for processing events.

If necessary, you can customize the columns by clicking the gear ⚙ icon.

Creating a report template

To create report template:

1. In the web interface, perform one of the following actions:

   - Under **Reports** → **Templates**, in the toolbar or menu ⋮, click **Create**.
   - Under **Resources** → **List**, in the toolbar or menu ⋮, click **New** and select **Report template**.

   The pane for creation a report template opens on the right.

2. In the **Template name** field, enter a name for the report template. The name must contain from 1 to 128 Unicode characters and must be unique within the selected tenant.

> The names of custom report templates must not match the names of predefined report templates in the Main tenant.

> When trying to create a report template with the same name as a predefined report template or assign the name of a predefined report template to a report template, the Main tenant returns an error. In other tenants you can create or duplicate a report template with the same name as a predefined report template. When creating report templates, we recommend using unique names.

3. In the **Template tenant** drop-down list, select the tenant that will own the report template being created.

4. In the **Collect data from tenants** drop-down list, select one or more tenants, based on the data of which reports will be generated.

5. If necessary, in the **Time period** drop-down list, select the time period from which you want to get analytics in one of the following ways:

   - If you want to specify an **exact date**, select start and end dates of the period in the calendar and click **Apply**.

     You can select a date up to and including the current date. The date and time format depends on your browser settings. If the **Range from** or **Range to** field has a value and you have not edited the time value manually, when you select a date in the calendar, the **Range from** field is automatically populated with `00:00:00,000`, and the **Date to** field is populated with `23:59:59,999`. If you have manually deleted the value in the **Range from** or **Range to** field, when you select a date in the calendar, the field is automatically populated with the current time. Once you select a value in one of the fields, the focus switches to the other field. If your **Range to** is earlier than your **Range from**, this earlier value is automatically inserted into the **Range from** field.

   - If you want to specify a **relative period**, select one of the periods available in the **Relative period** list.

     The period is calculated relative to the current time.

   - If you want to specify a **custom period**, set or edit the value of the **Range from** and **Range to** fields manually.

     You can enter an exact date and time in the `DD.MM.YYYY HH:mm:ss.SSS` format for the Russian localization and `YYYY-MM-DD HH:mm:ss.SSS` for the English localization or a period relative to the current time as a formula. You can also combine these methods. If you do not specify milliseconds when entering the exact date, `000` is substituted automatically. If you have edited the time in the **Range from** or **Range to** fields, picking a date in the calendar does not change the time component.

     In the relative period formulas, you can use the `now` parameter for the current date and time and the interval parameterization language: `+` (only in the **Range to** field), `-`, `/` (rounding to the nearest), as well as time units: `y` (year), `M` (month), `w` (week), `d` (day), `h` (hour), `m` (minute), `s` (second). For example, you can specify the period `now-5d` to get data for the last five days, or `now/w` to get data from the beginning of the first day of the current week (00:00:00:000 UTC) to the current time (`now`).

     > The **Range from** field is required, and its value cannot exceed the value of the **Range to** field, and also cannot be earlier than 1970-01-01 (if specifying an exact date or a relative period). The **Range to** cannot be earlier than the **Range from**. If you do not specify a value in the **Range to** from field, `now` is specified automatically.

By default, the **1 day** (`now-1d`) relative period is selected. The bounds of the period are included. For example, for **Today** time range, events are displayed from the beginning (00:00:00:000) of the current day to the current time (`now`) inclusive, and for **Yesterday** period, events are displayed from the beginning (00:00:00:000) of the previous day to 00:00:00:000 of the current day.

Kaspersky SIEM stores time values in UTC, but in the web interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the data display period, data will be displayed for the period from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative data display period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the **Range from** and **Range to** (if a value other than `now` is specified) by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want to display data for **Yesterday**, you need to change **Range from** to `now-1d/d-3h` and **Date to** to `now/d-3h`. If you want to display data for the **Today** period, you only need to change the value in the **Range from** field to `now/d-3h`.

> If you need results up to 23:59:59:999 UTC of yesterday, you can use an SQL query with a filter by Timestamp or specify an exact date and time.

6. If necessary, in the **Retention period** field, specify how long you want to store reports that are generated according to this template.

   The default value is 3 months.

7. If necessary, select tags for the report template from the **Tags** drop-down list.

8. If necessary, add a description of the report template.

9. Use the **CII status** toggle switch to enable the display of information for assets, alerts, and incidents related to critical information infrastructure (CII). In this case, reports in which the calculated data includes CII information, can be viewed only by users in whose settings the **Access to CII facilities** check box is selected.

   If this toggle switch is disabled, widgets of the reports do not display information for assets, alerts, and incidents related to critical information infrastructure (CII) even if the user has access to CII facilities.

10. Click **Save**.

    The report modification window opens.

11. If necessary, add the logo of the report template by dragging the image into the field or by clicking the **Upload a file** link. The image must be in JPG, PNG or GIF format. The maximum size of an image is 3 MB.

    The added logo will be displayed in the report instead of the solution logo.

12. Click the **Add widget** button and select a widget. This opens a window; in that window, configure the selected widget.

    You can add multiple widgets. You can drag widgets using the handle icon (⠿) in the widget's upper left corner. To resize the widget, use the stretch icon (⤡) that appears when you point to the lower right corner of the widget.

    The following limitations apply to widgets with the **Pie chart**, **Bar chart**, **Line chart**, **Counter** , and **Date Histogram** chart types:

    - In `SELECT` queries, you can use extended event schema fields of `String`, `Number`, and `Float` types.
    - In `WHERE` queries, you can use all types of extended event schema fields (`String`, `Number`, `Float`, `Array of strings`, `Array of numbers`, and `Array of floats`).

For widgets with the **Table** chart type, in `SELECT` queries, you can use all types of extended event schema fields (`String`, `Number`, `Float`, `Array of strings`, `Array of numbers`, and `Array of floats`).

By clicking the menu icon ⋮ in the upper right corner of the widget, you can change the settings of the widgets, copy and delete widgets.

13. Click **Create**.

A new report template is created. You can generate this report manually or schedule automatic report generation.

Managing report templates

This article describes how to modify and duplicate a report template, view its dependencies and versions, and delete a report template.

Editing report template

To edit report template:

1. In the web interface, go to one of the following sections:

   - **Reports** → **Templates**
   - **Reports** → **Generated reports**
   - **Resources** → **List**

     If you selected this section, you can select **Report template** for a more convenient display of objects in the **Resource kind** column.

2. Depending on the selected section, do one of the following:

   - If you have opened the **Reports** → **Templates** or **Resources** → **List** section, click the report template.

     Under **Resources** → **List**, you can click the change settings icon next to the name of the template you want.

   - If you have opened the **Reports** → **Generated reports** section, select the check box next to the name of the report whose template you want to change, and click the **Edit template** button

   The **Edit template** pane opens on the right.

3. Make the necessary changes.

4. Click **Save**.

The report template is changed.

Creating a report template based on an existing template

To create a copy of a report template:

1. In the web interface, go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**
     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.
2. Select the check box next to the report template you want to copy.
3. In the toolbar or in the menu (⋮), click **Duplicate**.
4. In the **Template settings** pane that opens, specify the settings for the report template to be created.
5. Click **Save**.

The report template is created based on the existing template.

Viewing dependencies

For each report template, you can open a dependency graph.

To view dependencies:

1. In the web interface, go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**
     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.
2. Select the check box next to the required report template.
3. In the toolbar or in the menu (⋮), click the **Show dependencies** button.
   A window with report template dependencies will be opened.
4. If you want to download the dependency data, click the **Download SVG** button.
5. If necessary, configure filters to display dependencies on the graph using the **Show on graph** drop-down list.

Viewing the version history

To view the version history of a report template:

1. In the web interface, go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.
2. Select the check box next to the report template for which you want to view versions.
3. In the toolbar or in the ⋮ menu, click **View versions history**.
4. If necessary, you can compare the versions with each other. To do this, select the check boxes next to the versions you want to compare and click **Compare**.
5. If you want to restore an earlier version of a template, select the check box next to the name of this template, click **Restore**, and then confirm the action.

Deleting report template

To delete a report template:

1. In the web interface, go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.
2. Select the check boxes next to the report templates you want to delete.
3. In the toolbar or in the menu (⋮), click **Delete**.
4. In the confirmation window that opens, do one of the following:
   - If you want to delete only the report template, click the **Delete** button.
   - If you want to delete a report template and all the reports that were generated using that template, click the **Delete with reports** button.

The report templates are deleted.

Exporting and importing report templates

You can export and import report templates.

Exporting a report template

Please consider the following factors when exporting report templates:

- Report templates are exported without tenant, storage, and space information because these parameters are configured for each instance of Kaspersky SIEM individually.
- Report template widgets are exported without tenant, storage, and space information.
- If before exporting you have deleted the predefined report template and created a custom report template with the same name as the predefined one, the date and time of export is appended to the name of the report template, for instance `Incidents Overview-2025-11-26 12:52:59`.

To export a report template:

1. In the web interface, go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.

   A table of all report templates that are available to you in Kaspersky SIEM is displayed.
2. In the toolbar or menu (⋮), click **Export**.
3. In the pane that opens perform the following actions:
   a. Enter the password for the file with exported resources. The password must satisfy the following requirements:
      - At least 16 characters.
      - At least one lowercase character.
      - At least one uppercase character.
      - At lease one numeral.
      - At least one special character.

   b. In the **Tenant** drop-down list, select the tenant from which you want to export the selected resources.

   c. Select the check boxes next to the resources you want to export.

      If you select the **All resources** check box, all resources in the selected tenant's folders will be exported.
4. Click the **Export** button.

Importing a report template

Please consider the following factors when importing report templates:

- If names of an imported report template and a report template that is already present in the tenant match, the report template is imported and the date and time of import is appended to the name, for instance `Incidents Overview-2025-11-26 12:52:59`.
- If a report template is imported into any tenant, the tenant of the imported report template is specified as the resource tenant and the data source tenant.
- Once a report template is imported, you need to specify spaces for widgets with events and, if necessary, expand the list of tenants.

To import a report template:

1. Open the KUMA web interface and go to one of the following sections:
   - **Reports** → **Templates**
   - **Resources** → **List**

     If you select this section, for easier viewing of objects in the **Resource kind** column, select **Report template**.

   A table of all report templates that are available to you in Kaspersky SIEM is displayed.
2. In the toolbar or menu (⋮), click **Import**.
3. In the sidebar, in the **Tenant** drop-down list, select the tenant to which you want to import the report template.
4. Select the import source: **File** or **Repository**.
5. Depending on the selected import source, follow these steps:
   - If you selected **File** as an import source:
     1. Specify the password for the imported file.
     2. Click the **Select file** button and select the file to import.
     3. Select the check boxes next to the templates that you want to import.
   - If you selected **Repository** as the import source, select one or more repository packages in the displayed table.
6. Click the **Import** button.

   If `exportID` of the imported report template and `exportID` of the report template that is already present in the tenant match, a conflict message is returned with suggestions on how to resolve the conflict:

   - **Skip**

     When this option is selected, all report templates selected for import are imported, except for the conflicting one.

- **Replace**.

  If this option is selected, the report template is imported and the data is overwritten.

If you want to look at the difference between report templates with the same `exportID`, you can click **Skip**, and then import the report template into another tenant and compare the report templates in different tenants.

7. If necessary, resolve conflicts between the report templates imported from the file and the existing ones.

Managing reports

This article describes how to generate, update, and delete a report.

Generating a report

You can generate a report manually or set up a schedule for automatic generation of reports.

To generate a report manually:

1. In the web interface, open the **Reports** section.
2. Do one of the following:
   - In the **Templates** tab:
     1. Select the check box next to the name of a report, that you want to generate.
     2. In the toolbar or menu (⋮), click **Launch report**.
   - On the **Generated reports** tab:
     1. Select the check box next to the name of a report, that you want to generate.
     2. In the toolbar or menu (⋮), click **Create report**.

The report is generated and displayed in the **Reports** → **Generated reports** section.

Report update

To update a generated report:

1. In the web interface, go to the **Reports** section and select **Generated reports**.
2. Select the check box next to the name of a report, that you want to update.
3. In the toolbar or menu (⋮), click **Create report**.

The report will be updated.

Report deletion

To delete report:

1. In the web interface, go to the **Reports** section and select **Generated reports**.
2. Select the check box next to the name of a report, that you want to delete.
3. In the toolbar or in the menu (⋮), click **Delete**.
4. Confirm report deletion in the window that opens.

   The selected report will be deleted.

Configuring report schedule

You can configure a schedule based on which the reports will be generated automatically and sent to the email addresses specified in settings.

If you want the generated reports to be sent by email, you need to configure an SMTP connection.

The report is not sent if it contains only widgets with errors. The report is sent if it contains at least one widget without errors.

To configure the report schedule:

1. In the web interface, go to the **Reports** → **Templates** section.
2. Select the check box next to the name of the report for which you want to configure a schedule.
3. Click the menu icon ⋮ and select **Edit schedule** from the drop-down list.
4. Enable the **Send report by schedule** toggle switch.
5. Under **Recur every**, specify the frequency of report generation.

   You can specify the frequency of generating reports by days, weeks, months, or years. Depending on the selected period, you should specify the time, day of the week, day of the month or the date of the report generation.
6. In the **Time** field, specify the report generation time.
7. In the **Timezone** drop-down list, select the time zone for the report generation time.
8. To send the generated report to email addresses, in the **Notification settings** section, do the following:

   a. In **the Notification template** drop-down list, select or create a notification template.

   b. In the **Send** section, click **Add**.

c. In the displayed pane, add the email addresses of the users and select the format:

- In the **Emails** drop-down list, specify email addresses of report recipients.
- In the **Format** drop-down list, select the report format: HTML, PDF, CSV, comma-separated CSV, or Excel.

You can add several user groups by clicking the **Add group** button.

Reports are sent to the specified email addresses each time a report is generated manually or according to a schedule.

If the recipients of an emailed report are Kaspersky SIEM users, they can download or view the report by clicking links in the email message. If the recipients are not Kaspersky SIEM users, they can follow the links but cannot log in to Kaspersky SIEM, so only attachments are available to them.

We recommend viewing HTML reports by clicking links in the web interface, because at some screen resolutions, the HTML report from the attachment may not be displayed correctly.

You can send an email without attachments. In this case, recipients will only be able to access reports via links and only after logging into Kaspersky SIEM (without role or tenant restrictions).

d. Click **Add**.

9. Click **Save**.

Report scheduling is configured.

Saving a report

To save generated reports in HTML and PDF formats, install the required packages on the device with the KUMA Core.

To save a report:

1. In the web interface, go to the **Reports** section and select **Generated reports**.
2. Do one of the following:
   - Select the check box next to the name of the report you want to save.
   - Click the name of the report. A report window with configured widgets opens.
3. In the **Save as** drop-down list, select a format: HTML, PDF, CSV, Split CSV, or Excel.

   If you want to save the report with complete data, select the CSV format.

   If the report contains a widget for which the **Totals** toggle switch is turned on and the widget displays the **Total** value, when the report is uploaded in CSV and extended CSV formats, the **Total** value is not displayed. To display the **Total** value in the report, you can use Excel formulas, copy and paste the total value from the widget, or use PDF or HTML attachments.

If a report contains widgets with identical names and you download the report in CSV or Excel format, the widget files are automatically renamed with a numeric suffix. Since renaming occurs automatically, when saving a report in different formats, the suffixes of renamed files for the same widget may not match across formats. For example, a `widget(2)` file in one format does not necessarily correspond to a `widget(2)` file in another format. For convenience, we recommend giving widgets unique names, regardless of the report format.

The report is saved to the folder specified in your browser settings.

Widgets

Widgets let you monitor the operation of the application. Widgets are organized into widget groups, each one related to the analytics type they provide. The following widget groups and widgets are available in KUMA:

- Events—widget for creating analytics based on events.
- Active lists—widget for creating analytics based on active lists of correlators.
- Alerts—group for alert analytics.

  The group includes the following widgets:

  - **Active alerts**—number of alerts that have not been closed.
  - **Active alerts by tenant**—number of unclosed alerts for each tenant.
  - **Alerts by tenant**—number of alerts of all statuses for each tenant.
  - **Unassigned alerts**—number of alerts that have the **New** status.
  - **Alerts by assignee**—number of alerts with the **Assigned** status, grouped by account name.
  - **Alerts by status**—number of alerts that have the **New**, **Opened**, **Assigned**, or **Escalated** status, grouped by status.
  - **Alerts by severity**—number of unclosed alerts grouped by their severity.
  - **Alerts by rule**—number of unclosed alerts grouped by correlation rule.
  - **Latest alerts**—table with information about the last 10 unclosed alerts belonging to the tenants selected in the layout.
  - **Alerts distribution**—number of alerts created during the period configured for the widget.
- Assets—group for analytics for assets from processed events. This group includes the following widgets:

  - **Affected assets**—table with information about the level of importance of assets and the number of unclosed alerts they are associated with.
  - **Affected asset categories**—categories of assets linked to unclosed alerts.
  - **Number of assets**—number of assets that were added to KUMA.

- **Assets in incidents by tenant**—number of assets associated with unclosed incidents. The grouping is by tenant.
- **Assets in alerts by tenant**—number of assets associated with unclosed alerts, grouped by tenant.

- Incidents—group for incident analytics.

  The group includes the following widgets:

  - **Active incidents**—number of incidents that have not been closed.
  - **Unassigned incidents**—number of incidents that have the **Opened** status.
  - **Incidents distribution**—number of incidents created during the period configured for the widget.
  - **Incidents by assignee**—number of incidents with the **Assigned** status, grouped by user account name.
  - **Incidents by status**—number of incidents grouped by status.
  - **Incidents by severity**—number of unclosed incidents grouped by their severity.
  - **Active incidents by tenant**—number of unclosed incidents grouped by tenant available to the user account.
  - **All incidents**—number of incidents of all statuses.
  - **All incidents by tenant**—number of incidents of all statuses, grouped by tenant.
  - **Affected assets in incidents**—number of assets associated with unclosed incidents.
  - **Affected assets categories in incidents**—asset categories associated with unclosed incidents.
  - **Affected users in Incidents**—users associated with incidents.
  - **Latest incidents**—table with information about the last 10 unclosed incidents belonging to the tenants selected in the layout.

- **Event sources**—group for event source analytics. The group includes the following widgets:

  - **Top event sources (value in DeviceProduct field) by number of base events collected in correlation events** displays the number of base events collected in correlation events and grouped by data sources specified in the DeviceProduct field.
  - **Top event sources (value in DeviceProduct field) by convention rate** displays the ratio of the number of base events in correlation events and the total number of base events grouped by data sources specified in the DeviceProduct field.

    In some cases, the number of correlation events generated by sources may be inaccurate. To obtain accurate statistics, it is recommended to specify the Device Product event field as unique in the correlation rule, and enable storage of all base events in a correlation event. However, correlation rules with these settings consume more resources.

- Users—group for analytics related to users from processed events. The group includes the following widgets:
  - **Affected users in alerts**—number of accounts related to unclosed alerts.
  - **Number of AD users**—number of Active Directory accounts received via LDAP during the period configured for the widget.
- Image—a widget for displaying an uploaded image on the dashboard or in the report.
- Text—a widget for displaying arbitrary text on the dashboard or in the report.

> In the events table, in the event details area, in the alert window, and in the widgets, the names of assets, accounts, and services are displayed instead of the IDs as the values of the `SourceAssetID`, `DestinationAssetID`, `DeviceAssetID`, `SourceAccountID`, `DestinationAccountID`, and `ServiceID` fields. When exporting events to a file, the IDs are saved, but columns with names are added to the file. The IDs are also displayed when you point the mouse over the names of assets, accounts, or services.
>
> Searching for fields with IDs is only possible using IDs.

Basics of managing widgets

The principle of data display in the widget depends on the type of the graph. The following graph types are available in KUMA:

- Pie chart ( ).
- Counter ( ).
- Table ( ).
- Bar chart ( ).
- Date Histogram ( ).
- Line chart
- Stacked Bar chart
- Speedometer chart.

Basics of general widget management

The name of the widget is displayed in the upper left corner of the widgets. By clicking the link with the name of the widget about events, alerts, incidents, or active lists, you can go to the corresponding section of the KUMA web interface.

A list of tenants for which data is displayed is located under the widget name.

In the upper right corner of the widget, the period for which data is displayed on the widget is indicated (for example, 30 days `30д`). Keep in mind that the data displayed in the dashboard may lag behind real time because of caching. You can view the date and time of the last update by hovering over the period icon.

If the **Show data for previous period** setting is enabled for the widget, and the widget is displaying data for a relative period, the tooltip also displays the previous period. The previous period is calculated relative to the current period as start and end values of the current period minus the duration of the current period. For example, if data is updated daily and displayed for a month, but only the first 10 days of the month have passed, the previous period is taken to be the last 10 days of the previous month.

You can change the data display period for the widget by clicking the period icon and selecting an exact date or a relative period in the window that is displayed. If you want the widget to display data for the period selected for the layout, click the **Reset** button. Changing the displayed period on the layout also changes the period displayed in the widget.

> The time in the widget is displayed in the local time zone set in the browser.

The **CSV** button is located to the left of the period icon. You can download the data displayed on the widget in CSV format (UTF-8 encoding). The downloaded file name has the format <widget name>_<download date (YYYYMMDD)>_<download time (HHMMSS)>.CSV.

The widget displays data for the period selected in widget or dashboard settings only for the tenants that are selected in widget or dashboard settings.

If you have enabled the **Show total** toggle switch in the widget settings, the widget displays the **Total** value, but when you download the widget in CSV format, the **Total** value is not displayed. To display the **Total** value in the report, you can use Excel formulas or manually copy the total value from the widget.

Basics of managing Pie chart graphs

A pie chart with a legend is displayed below the list of tenants. The legend lists the names of the categories corresponding to the sectors of the diagram. By left-clicking a category in the legend, you can go to the section of the KUMA web interface with the corresponding data. The data in that section is sorted in accordance with the filters and/or search query specified in the widget.

When going from the legend of the widget to the events details section, pay attention to the text of the legend item that you click to go to the events section. Any \ or ' characters used in the text are escaped in the text of the SQL query. However, the / character is not escaped.

If the request returns data subdivided into a large number of sectors, then the **Other** sector is added to optimize the display of the widget. You can make the **Other** sector smaller by making a more detailed query. You can use `LIMIT` and `WHERE` clauses to refine your query.

Under the period icon, the number of events, active lists, assets, alerts, or incidents grouped by the selected criteria for the data display period will be displayed.

Examples:

- In the **Alerts by status** widget, under the period icon, the number of alerts grouped by the **New**, **Open**, **Assigned**, or **Escalated** status is displayed.
  If you want to see the legend only for alerts with the **Opened** and **Assigned** status, you can clear the check boxes to the left of the **New** and **Escalated** statuses.
- In the **Events** widget, for which the SQL query `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10` is specified, 10 events are displayed below the period icon, grouped by name and sorted in descending order.
  If you want to view events with specific names in the legend, you can clear the check boxes to the left of the names of events that you do not want to see in the legend.

Basics of managing Counter graphs

Graphs of this type display the sum total of selected data.

Example 1:
The **Number of assets** widget displays the total number of assets added to KUMA.
Example 2:
If you want to view trends to compare current data with data for a past period, you can create a widget that displays upward or downward trends. Trends can be configured in the following widgets:

- **Assets → Number of assets**.
- **Assets → Customized widget**.
- **Alerts → Active alerts**.
- **Alerts → Unassigned alerts**.
- **Incidents → Active incidents**.
- **Incidents → Unassigned incidents**.
- **Incidents → All incidents**.
- **Users -> Number of AD users**.
  To configure the display of trends, you need to enable the **Show data for previous period** toggle switch, and then select a trend on the **Appearance** tab. If the percentage value cannot be calculated, or if the values are equal, the — icon is displayed. If **Up is better** is selected, an uptrend is indicated by a green arrow on the chart, and a downtrend is indicated by a red arrow. If **Down is better** is selected, an uptrend is indicated by a red arrow on the chart, and a downtrend is indicated by a green arrow.
  You can click the value to change the display of data in the widget (for example, to display absolute values instead of percentages). This functionality is available when the widget is displayed on the dashboard and when the TV mode is on.

Basics of managing Table graphs

Graphs of this type display data in a table format.

Example:
In the **Events** widget, for which the SQL query `SELECT TenantID , Timestamp , Name , DeviceProduct , DeviceVendor FROM `events` LIMIT 10` is specified, displays an event table with **TenantID**, **Timestamp**, **Name**, **DeviceProduct**, and **DeviceVendor** columns. The table contains 10 rows.

You can customize the display of data in the table using two-color (red and green) or three-color (red, yellow, and green) gradient fill. After selecting the type of gradient, you can adjust the direction of the fill by clicking the toggle direction icon (⇆) and set thresholds. Two values must be specified for a two-color gradient, and three for a three-color gradient. These values are displayed in the legend and determine the color of the marker added to the cell of the selected column. The column is specified in the **Field for gradient indicator** drop-down list.

Basics of managing Bar chart graphs

A bar chart with a legend is displayed below the list of tenants. The legend lists the names of the categories corresponding to the bars of the diagram. By left-clicking a category in the legend, you can go to the section of the KUMA web interface with the corresponding data. The data in that section is sorted in accordance with the filters and/or search query specified in the widget.

When going from the legend of the widget to the events details section, pay attention to the text of the legend item that you click to go to the events section. Any \ or ' characters used in the text are escaped in the text of the SQL query. However, the / character is not escaped.

If the request returns data subdivided into a large number of bars, then the **Other** bar is added to optimize the display of the widget. You can make the **Other** bar smaller by making a more detailed query. You can use `LIMIT` and `WHERE` clauses to refine your query.

Example:
In the **a Netflow top internal IPs** widget for which the SQL query `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10` is specified, the x-axis of the chart corresponds to the total traffic in bytes, and the y-axis corresponds to destination port addresses. The data is grouped by destination address in descending order of total traffic.

You can also customize the display of bars using two-color (red and green) or three-color (red, yellow, and green) gradient fill. After selecting the type of gradient, you can adjust the direction of the fill by clicking the toggle direction icon (⇆) and set thresholds. Two values must be specified for a two-color gradient, and three for a three-color gradient. These values are displayed in the legend and determine the coloring of the bars.

Basics of managing Date Histogram graphs

A Date Histogram with a legend is displayed below the list of tenants. The legend lists the names of the categories corresponding to the bars of the diagram. By left-clicking a category in the legend, you can go to the section of the KUMA web interface with the corresponding data. The data in that section is sorted in accordance with the filters and/or search query specified in the widget.

When going from the legend of the widget to the events details section, pay attention to the text of the legend item that you click to go to the events section. Any \ or ' characters used in the text are escaped in the text of the SQL query. However, the / character is not escaped.

If, when creating a widget with a **Date Histogram** type, the **Bar chart** view is selected, you can customize the display of the bars using two-color (red and green) or three-color (red, yellow, and green) gradient fill. After selecting the type of gradient, you can adjust the direction of the fill by clicking the toggle direction icon (⇆) and set thresholds. Two values must be specified for a two-color gradient, and three for a three-color gradient. These values are displayed in the legend and determine the coloring of the bars.

Example:

```
SELECT count(ID) AS `metric`, Timestamp AS `value`
FROM `events`
GROUP BY Timestamp
ORDER BY `metric` DESC
LIMIT 250
```

The X axis of the chart shows the date when the event was created, and the Y axis shows the number of events. The bars of the chart are arranged from left to right in descending order of the number of events.

If an additional field with the `category` alias is used in the SQL query, the bar chart is displayed as a stacked bar chart. In this case, gradient fill is not applied.

Example:

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, Type AS `value`
FROM `events`
GROUP BY Timestamp, Type
ORDER BY metric DESC
LIMIT 250
```

The X axis indicates the time intervals, and the Y axis indicates the number of events. Each segment of the bar corresponds to a value of the field marked as `Type`.

If, when creating a widget with a **Date Histogram** type, the **Line chart** view is selected, there are two options for displaying the chart: single line (if only the `metric` and `value` fields are specified in the query) and multiple lines (if an additional field with the `category` alias is used). This lets you compare values for different groups, depending on which field is used for grouping in the query. For example, correlation rules, users, or hosts can be used. No gradient fill is applied to such charts.

Example of a query to display a line chart with multiple lines

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, CorrelationRuleName AS `value`
FROM `events`
WHERE Type = 3
GROUP BY Timestamp, CorrelationRuleName
ORDER BY metric DESC
LIMIT 250
```

The chart displays the intervals on the X-axis (the field specified as the `category`). The Y-axis displays the number of times the correlation rules were triggered (the field marked as `metric`). Each line on the chart corresponds to a unique value in the `value` field (in this case, the name of the correlation rule).

You can use the following time fields for grouping in a Date Histogram:

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> For convenience, we recommend using supported ClickHouse functions to round the values in the time field (`Timestamp`), for example, to 1 hour or 1 day.

For a **Date Histogram** widget with the **Line chart** view, you can also configure the display of the average value. To do this, on the **Appearance** tab, for the **Regression** setting, select **LOESS**.

Basics of managing Line chart graphs

A line chart with a legend is displayed below the list of tenants. The legend displays the names of the categories corresponding to the lines on the chart. By left-clicking a category in the legend, you can go to the section of the KUMA web interface with the corresponding data. The data in that section is sorted in accordance with the filters and/or search query specified in the widget.

When going from the legend of the widget to the events details section, pay attention to the text of the legend item that you click to go to the events section. Any \ or ' characters used in the text are escaped in the text of the SQL query. However, the / character is not escaped.

Example:
In the **Events** widget, for which the SQL query `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250` is specified, the x-axis corresponds to the approximate port number, and the y-axis corresponds to the number of events. The data is grouped by port number in ascending order.

For a **Line chart** widget, you can also configure the display of the average value. To do this, on the **Appearance** tab, for the **Regression** setting, select **Linear**. If the chart displays multiple categories, the average is displayed for each category.

Basics of managing graphs of the Stacked bar chart type

A stacked bar chart with a legend is displayed below the list of tenants. The legend displays the names of the categories that make up parts of each bar. To the left of each category is a check box that lets you hide or show the category. The number of bars in the chart corresponds to the number of values in the selected grouping. The bars have captions. The color of the corresponding category in the bar is assigned automatically. When you hover over the zones of the bars, a tooltip is displayed with the value and a description of the value. You can left-click a category in the legend to go to the section of the KUMA web interface with the relevant data.

When going from the legend of the widget to the events details section, pay attention to the text of the legend item that you click to go to the events section. Any \ or ' characters used in the text are escaped in the text of the SQL query. However, the / character is not escaped.

The meaning of bar height depends on the **Format** setting:

- If the **Absolute values** format is configured, the height of the bars corresponds to the sum of the values of the measured figure.
- If the **Relative values, %** format is configured, all bars have the same height of 100%, and the relative heights of colored zones on the bars correspond to the ratios of the values.

If, when creating a custom widget based on the stacked bar chart, you selected the **Show data for previous period** option, and the standard `value`, `category`, `metric` aliases are used in the query, the chart displays previous-period data as separate bars. However, if instead of the standard `metric`, the query uses a custom metric calculation with non-standard aliases, the **Show data for previous period** is not taken into account when displaying the chart (see example queries below).

Examples:

When creating a custom widget of the **Stacked bar chart** type based on an SQL query of an **Events** widget, the following rules apply:

- The field in the query that is marked as the `value` alias (required field) is used in the chart as the field by which the legend is created and the bars are divided into categories.
- The field in the query that is marked as the `category` alias (required field) is used in the chart as the field that defines the arrangement of bars along the X axis.
- The field in the query marked as the `metric` alias is used in the chart as the field that defines how bar areas are counted. In this case, the distribution is performed automatically.

However, you can manage the count by using standard aggregation functions (`sum`, `avg`, `min`, `max`, `count`) and your own arbitrarily named aliases as metrics instead of the standard `metric` alias (in this case, the display of data for the previous period is not supported).

Example 1:

For the **Events** widget, the following SQL query is specified with standard aliases, and the **Show data for previous period** option was selected when creating the widget:

```
SELECT count(ID) AS `metric`,
       Type AS `value`,
       TenantID AS `category`
FROM `events`
GROUP BY value, category
ORDER BY metric DESC
```

The X-axis stands for tenants (the field marked as the `category`), the Y-axis stands for the number of events of a certain type (the field marked as the `value`). Inside each bar, the quantity corresponding to a certain type is represented by a certain color. In the legend, the names of the event types by which the bars are divided are displayed as categories. Each category has an automatically assigned corresponding color on the bar. If you want to view only certain event types in the chart, you can clear or select the check boxes to the left of the corresponding event types in the legend.

Next to each bar, an additional bar is displayed with historical data, if such data was received in the query response.

Example 2:

For the **Events** widget, the following SQL query is marked with custom metrics marked as the `Base` and `Audit` aliases instead of the standard `metric` alias:

```
SELECT SUM(IF (Type = 1,1,0)) AS `Base`,
       SUM(IF (Type = 4,1,0)) AS `Audit`,
       TenantID as `category`
FROM `events`
GROUP BY category
```

The X-axis stands for tenants (the field marked as `category`), the Y-axis stands for the number of events of each type (custom metrics marked as the `Base` and `Audit` aliases). Inside each bar, the quantity corresponding to a certain metric is represented by a certain color. In the legend, the `Base` and `Audit` metrics by which the bars are divided into categories are displayed as category names. Each category has an automatically assigned corresponding color on the bar. If you want to view only event corresponding to a certain metric in the chart, you can clear or select the check boxes to the left of the relevant metric in the legend.

The additional bar with historical data is not displayed for a query with custom metrics, even if the **Show data for previous period** option was selected when creating the widget.

Example 3:

For the **Events** widget, the following SQL query is specified with standard aliases:

```
SELECT count(ID) AS `metric`,
       TenantID as `value`,
       Type as `category`
FROM events
GROUP BY value, category
ORDER BY metric DESC
```

In contrast to the similar query in example 1, in this case, the X-axis stands for the types of events (the field marked as the `category`), and the tenants (the field marked as the `value`) are represented by ranges of values in the bars (along the X axis) and the corresponding captions in the legend.

Example 4:

For the **Events** widget, the following SQL query is specified with standard aliases:

```
SELECT count(ID) AS `metric`,
       CAST(fromUnixTimestamp64Milli(Timestamp) AS DATE) AS `category`,
       Type as `value`
FROM `events`
GROUP BY category, value
ORDER BY category DESC
```

The chart displays the days of the month on the X axis (the field marked as the `category`). The Y axis displays the number of events of a particular type (the field marked as the `value`).

To create a similar chart with bars arranged by date and/or time, use a query with grouping and sorting by the following fields of the `timestamp` type:

- `Timestamp`
- `DeviceCustomDate1`

- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

We recommend using the **Date Histogram** to work with data that is arranged by date and/or time.

Basics of managing Speedometer charts

This type of chart displays the percentage of the number of objects of the selected category vs the total number of objects for a certain period. The **Speedometer chart** can be used for the following objects:

- Assets in a category that satisfy certain criteria vs the total number of assets in the same category or uncategorized assets
- Alerts that satisfy certain criteria vs the total number of alerts for a certain period
- Incidents that satisfy certain criteria vs the total number of incidents
- Events that satisfy certain criteria vs the total number of events for a certain period

The value on the chart is displayed as a percentage with a color matching the configured ranges of values. By default, the following ranges are specified: 0–30, 30–70, 70–100.

Example 1:
In the **Assets** customized widget, the user selects an asset category for comparing the number of assets in it with the total number of assets. The user can specify threshold values for the scale on the graph. Then, based on one or more conditions for the Y-axis, a calculation is performed with the existing asset database.
Example 2:
In the **Alerts** widget, you can select the **Speedometer chart** chart type for the **Active alerts** and **Unassigned alerts** categories. For alerts, a tenant and a period for analysis are selected. By default, these values match the values specified in the relevant dashboard. In the total number of alerts, you can also view data for the previous period.
The percentage value for the **Active incidents** and **Unassigned incidents** categories is calculated in the same way in the **Incidents** widget.
Example 3:
In the **Events** widget, for the **Speedometer chart** chart type, the user specifies a tenant, a period for analysis, and the event data storage. The SQL query is displayed as follows:

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

Special considerations for displaying data in widgets

Limitations for the displayed data

For improved readability, KUMA has limitations on the data displayed in widgets depending on its type:

- Pie chart displays a maximum of 20 slices.
- Bar chart displays a maximum of 40 bars.
- Table displays a maximum of 500 entries.
- Date histogram displays a maximum of 365 days.

Data that exceeds the specified limitations is displayed in the widget in the **Other** category.

You can download the full data used for building analytics in the widget in CSV format.

Summing up the data

The format of displaying the total sum of data on date histogram, bar chart and pie chart depends on the locale:

- English locale: decades (every three digits) are separated by commas, the decimal part is separated by a period.
- Russian locale: decades (every three digits) are separated by spaces, the decimal part is separated by a comma.

Managing widgets

Creating a widget

You can create a widget on a dashboard while creating or editing the dashboard.

To create a widget:

1. Create a dashboard or switch to the selected dashboard editing mode.
2. Click **Add widget**.
3. Select a widget type from the drop-down list.
   This opens the widget settings window.
4. Edit the widget settings.

5. If you want to see how the data will be displayed in the widget, click the **Update preview** button.
6. Click **Save** in the widget settings window.
   The widget appears on the dashboard.
7. Click the **Save** button in the dashboard settings window.

Editing a widget

To edit widget:

1. In the KUMA web interface, select the **Dashboards** section.
2. Expand the list of dashboards in the upper left corner of the window.
3. Select a dashboard and click the **Edit** button.
   This opens the dashboard settings window.
4. On the widget that you want to edit, click the menu (⋮) icon.
5. Select **Edit**.
   This opens the widget settings window.
6. Edit the widget settings.
7. Click **Save** in the widget settings window.
8. Click the **Save** button in the dashboard settings window.

The changes are applied to the widget.

Deleting a widget

To delete a widget:

1. In the KUMA web interface, select the **Dashboards** section.
2. Expand the list of dashboards in the upper left corner of the window.
3. Select a dashboard and click the **Edit** button.
   This opens the dashboard settings window.
4. On the widget that you want to delete, click the menu icon ⋮.
5. Select **Delete**.

6. This opens a confirmation window; in that window, click **OK**.

7. Click the **Save** button.

The widget is deleted.

Widget settings

This section describes the settings of all widgets available in KUMA.

Events widget

You can use the **Events** widget to get analytics based on SQL queries.

When creating this widget, you must specify the settings described in the tables below.

General tab

The following table describes the settings on the **General** tab.

Description of parameters

Parameter	Description
Name	Name of the widget. When saving a report in Excel format, the name of the widget displayed in the header of the sheet is limited to 31 characters. We recommended keeping this limitation in mind when naming widgets.
Graph	Graph type. The following graph types are available: • **Pie chart**. • **Bar chart**. • **Counter**. • **Line chart**. • **Table**. • **Date Histogram**. • **Stacked bar chart** • **Speedometer chart**
Format	Data display format: **Absolute values** or **Relative values, %**. The setting is available for a **Stacked bar chart**. If you select the **Absolute values** format, the heights of the bars correspond to the sum of the values of the measured indicator. If you select the **Relative values, %** format, all bars have the same height of 100%, and the relative heights of colored zones on the bars correspond to the ratios of indicator values. By default, **Absolute values** is selected.
Timeline view	Time data display format: **Bar chart** or **Line chart**. This setting is available for charts of the **Date Histogram** type. When you select the **Bar chart** format, the data is displayed as vertical bars by default. If the SQL query contains an additional field with the `category` alias, the chart becomes a stacked bar chart, that is, each bar is divided into stripes in accordance with the values of this field. When you select the **Line chart** format, the data is displayed as one or more (depending on the query) polylines drawn through points on the time axis. The **Bar chart** format is selected by default.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Time interval	Period for which data is displayed in the widget. The default is **As layout**, meaning that data is displayed for the period selected for the layout. You can also specify a period for the widget in one of the following ways: • Select the exact start and end date and time of the period in the calendar and click **Apply**. • Select a period relative to the present time in the **Relative period** list. • Specify a value manually: select an exact date and time or a relative period, or a combination of both. For details, see the *Configuring a period* subsection below.

Parameter	Description
Show data for previous period	Enable the display of data for two periods at the same time: for the current period and for the previous period. When using a **Stacked bar chart**, the **Show data for previous period** setting is taken into account if the query contains standard aliases: `value`, `category`, `metric`. However, if instead of the standard `metric`, the query uses a custom metric calculation with non-standard aliases, the **Show data for previous period** is not taken into account.
Defined variables	Local or global variables that you can use to filter widget data. Then click the **Add** button. If you are adding a local variable, enter an arbitrary name for the variable, then enter the value of the variable. If you are adding a global variable, in the list, select the name of the variable that you specified in the dashboard properties.
Storage	Storage that is searched for events. The list displays the available spaces. You can select only one storage, but you can select one or more spaces. The values in the **Storage** field are independent of the selected tenants in the **Tenant** field. The field displays storages and spaces, like in the **Events** section.When a new space is created in the storage, this new space is not selected by default in the widget settings. You must manually select the new space. If the user has access to all spaces listed in the widget, the widget can display the event information for tenants specified in the space set in the user's permissions. If the user does not have access rights to one or more spaces of the storage, the widget cannot display information; the user cannot edit the widget, but can duplicate the widget using the **Duplicate** button. Duplication does not depend on access rights to spaces. If a template is duplicated in widgets that have spaces specified that are not accessible to the user, the value in the **Storage** field is reset. Such widgets display an error: Access denied (Operation returns no results because of allowed and selected event spaces). To save the template, you need to specify spaces in widgets. In widgets that have spaces that are accessible to the user, the value of the **Storage** field is not reset and is saved when the template is duplicated. When the user downloads the template, the data of inaccessible files are hidden in the downloaded file. If the user's email address is included in the list of recipients of the scheduled report, the user gets the full version of the report, regardless of which spaces are accessible.

Parameter	Description

SQL query field	Query for filtering and searching for events manually. You can create a query in Builder by clicking **Use sql builder**.
	You can use extended event schema fields to create a chart of the **Table** type.
	Example
	Prerequisite:
	
	Events are coming from a FWSaaS system.
	
	10.08.2023 12:12:12 src=10.10.10.10 ReqUrls=[https://google.com, https:/ya.ru]
	
	10.08.2023 12:12:23 src=10.10.10.20 ReqUrls=[https://google.com, https:/yndex.ru]
	
	10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru]
	
	The KUMA Main administrator has added an extended event schema field in KUMA in the **Settings** → **Other** → **Advanced event schema fields** section. At the KUMA normalizer, field mapping is configured for the **ReqUrls** and **SA.urls** fields.
	
	In KUMA, normalized events look as follows:
	
	DeviceReceiptTime=10.08.2023 12:12:12 SourceAddress=10.10.10.10 SA.urls=[https://google.com, https:/ya.ru]
	
	DeviceReceiptTime=10.08.2023 12:12:23 SourceAddress=10.10.10.20 SA.urls=[https://google.com, https:/yandex.ru]
	
	DeviceReceiptTime=10.08.2023 12:12:30 SourceAddress=10.10.10.30 SA.urls=[https://google.com, https:/ya.ru, https://mail.ru]
	
	You want to build a "Top URLs for 30 minutes" dashboard. Here is an example of a request in the **Events** section and in widgets:
	
	SELECT res.1 AS url, res.2 AS count FROM (SELECT arrayJoin(groupArray((url, count))) AS res FROM (SELECT url, count() AS count FROM (SELECT SA.urls AS urls FROM `events`) ARRAY JOIN urls AS url GROUP BY url) GROUP BY url)
	
	Result:
	
	url count
	
	google.com 3
	
	ya.ru 2
	
	mail.ru 1
	
	yandex.ru 1
	
	KUMA supports the following functions that allow using arrays in queries:
	• The `groupArray` function packs all values of the x argument into an array and is used in aggregate functions when grouping data.
	• The `arrayJoin` function expands the array into separate strings as a result of the query.
	You can use variables in the SQL query. You can specify variables only when creating the query manually. You cannot use variables in the SQL builder.
	Example with variables
	`Example SQL query with a local variable`
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	This query uses the local variable `$Name`. The value of the `Name` event field is substituted into this variable. You can apply the variable by clicking the funnel icon ( ) on the widget. This opens a window; in that window, you can specify a value for the variable. The widget filters the selection by the selected value of the `Name` field.
	
	Note that if in the SQL query you specify a variable for a field that takes a numeric value, such a value must be converted to a string. You can do this using the `toString` function. Otherwise, the SQL query returns an error.
	
	`Example`
	`SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	In this query, the `SourcePort` event field has a numeric value, therefore it is converted to a string: `toString(SourcePort)`.
	
	For detailed information on creating an SQL query in the query constructor, see below.
	
	The following limitations apply:
	• The `metric` and `value` aliases in SQL queries cannot be edited for any type of event analytics widget, except tables.
	• Aliases in widgets with charts of the **Table** type can contain Latin and Cyrillic characters, as well as spaces. When using spaces or Cyrillic, the alias must be enclosed in quotation marks: `"An alias with a space"`, `` `Another alias` ``.
	• `ARRAY JOIN SQL` queries are not supported.
	• When displaying data for the previous period, sorting by the `count(ID)` parameter may not work correctly. It is recommended to sort by the `metric` parameter. For example, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.

Parameter	Description
	• In widgets with charts of the **Counter** type, you must specify the method of data processing for the values of the `SELECT` function: `count`, `max`, `min`, `avg`, `sum`. • In widgets with charts of the **Table** type, the gradient is drawn based on the values of a number or time field (for example, `Timestamp`) specified in the SQL query. This field can be selected from the **Field for gradient indicator** drop-down list (if the query contains multiple number or time fields, any one of these can be selected). After this, the cells of the selected column are highlighted with gradient fill markers. If a field is not present in the query, the **Appearance** tab does not display the **Gradient** and **Field for gradient indicator** fields. • In **Stacked bar chart** widgets, `Timestamp` values are not displayed on the x-axis when using a standard query. If you want to display time along the X axis, we recommend using a **Line chart**. If you need to use a **Stacked bar chart**, the `Timestamp` value must be converted to string: `toString(Timestamp) AS `category``.

Configuring a period

To configure the data display period, do one of the following:

- If necessary, change the date and time in the **Time period** setting in one of the following ways:

  - If you want to specify an **exact date**, in the calendar, select the start and end date of the period and click **Apply**.

    You can select a date up to and including the current date. The date and time format depends on your browser settings. If the **Range from** or **Range to** field has a value and you have not edited the time value manually, when you select a date in the calendar, the **Range from** field is automatically populated with `00:00:00,000`, and the **Date to** field is populated with `23:59:59,999`. If you have manually deleted the value in the **Range from** or **Range to** field, when you select a date in the calendar, the field is automatically populated with the current time. Once you select a value in one of the fields, the focus switches to the other field. If your **Range to** is earlier than your **Range from**, this earlier value is automatically inserted into the **Range from** field.

  - If you want to specify a **relative period**, select one of the periods available in the **Relative period** list.

    The period is calculated relative to the current time.

  - If you want to specify a **custom period**, set or edit the value of the **Range from** and **Range to** fields manually.

    You can enter an exact date and time in the `DD.MM.YYYY HH:mm:ss.SSS` format for the Russian localization and `YYYY-MM-DD HH:mm:ss.SSS` for the English localization or a period relative to the current time as a formula. You can also combine these methods. If you do not specify milliseconds when entering the exact date, `000` is substituted automatically. If you have edited the time in the **Range from** or **Range to** fields, picking a date in the calendar does not change the time component.

    In the relative period formulas, you can use the `now` parameter for the current date and time and the interval parameterization language: `+` (only in the **Range to** field), `-`, `/` (rounding to the nearest), as well as time units: `y` (year), `M` (month), `w` (week), `d` (day), `h` (hour), `m` (minute), `s` (second). For example, you can specify the period `now-5d` to get data for the last five days, or `now/w` to get data from the beginning of the first day of the current week (00:00:00:000 UTC) to the current time (`now`).

    > The **Range from** field is required, and its value cannot exceed the value of the **Range to** field, and also cannot be earlier than 1970-01-01 (if specifying an exact date or a relative period). The **Range to** cannot be earlier than the **Range from**. If you do not specify a value in the **Range to** from field, `now` is specified automatically.

  Kaspersky SIEM stores time values in UTC, but in the web interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the data display period, data will be displayed for the period from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative data display period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the **Range from** and **Range to** (if a value other than `now` is specified) by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want to display data for **Yesterday**, you need to change **Range from** to `now-1d/d-3h` and **Date to** to `now/d-3h`. If you want to display data for the **Today** period, you only need to change the value in the **Range from** field to `now/d-3h`.

> If you need results up to 23:59:59:999 UTC of yesterday, you can use an SQL query with a filter by Timestamp or specify an exact date and time.

The bounds of the period are inclusive: for example, for the **Today** time range, events are displayed from the beginning (00:00:00:000 UTC) of the current day to the current time (**now**) inclusive, and for the **Yesterday** period, events are displayed from the beginning (00:00:00:000 UTC) of the previous day to 00:00:00:000 UTC of the current day. You can view the date and time of the last data update and the exact period for which the data is displayed by hovering over the period icon in the widget.

If the **Show data for previous period** setting is enabled for the widget, and the widget is displaying data for a relative period, the tooltip also displays the previous period. The previous period is calculated relative to the current period as start and end values of the current period minus the duration of the current period. For example, if data is updated daily and displayed for a month, but only the first 10 days of the month have passed, the previous period is taken to be the last 10 days of the previous month.

- If you want the widget to display data for the period selected for the layout, click the **Reset** button. Changing the displayed period on the layout also changes the period displayed in the widget.

How to create a query in Builder

To create a query in Builder:

1. Specify the values of the following parameters:

   a. **SELECT**—event fields that should be returned. The number of available fields depends on the selected graph type.

      - In the drop-down list on the left, select the event fields for which you want to display data in the widget.
      - The middle field displays what the selected field is used for in the widget: **metric** or **value**.

        > If you selected the **Table** graph type, in the middle fields, you must specify column names using ANSII-ASCII characters.

      - In the drop-down list on the right, you can select an operation to be performed on the data:
        - **count**—event count. This operation is available only for the **ID** event field. Used by default for line charts, pie charts, bar charts, and counters. This is the only option for date histogram.
        - **max** is the maximum value of the **event** field from the event selection.
        - **min** is the minimum value of the **event** field from the event selection.
        - **avg** is the average value of the **event** field from the event selection.
        - **sum** is the sum of event field values from the event selection.

b. **SOURCE** is the type of the data source. Only the **events** value is available for selection.

c. **WHERE**—conditions for filtering events.

- In the drop-down list on the left, select the event field that you want to use for filtering.
- Select the necessary operator from the middle drop-down list. The available operators depend on the type of value of the selected event field.
- In the drop-down list on the right, enter the value of the condition. Depending on the selected type of field, you may have to manually enter the value, select it from the drop-down list, or select it on the calendar.

You can add search conditions by clicking **Add condition** or remove search conditions by clicking ×.

You can also add groups of conditions by clicking **Add group**. By default, groups of conditions are added with the **AND** operator, but you can change the it if necessary. Available values: **AND**, **OR**, **NOT**. Group conditions are deleted using the **Delete group** button.

d. **GROUP BY**—event fields or aliases to be used for grouping the returned data. This parameter is not available for **Counter** graph type.

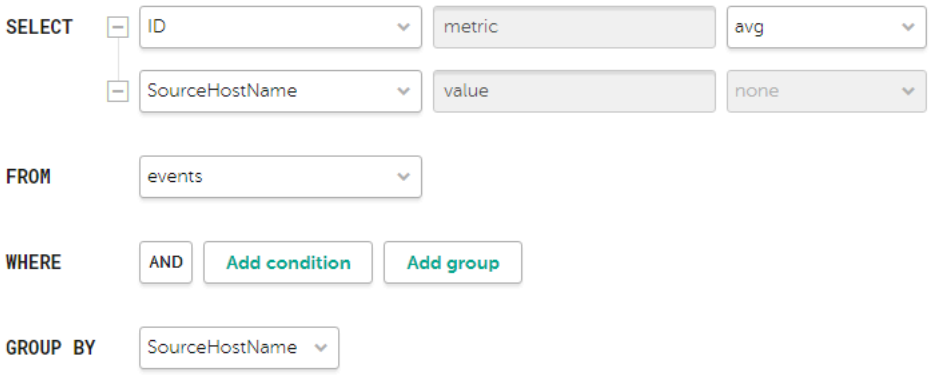
e. **ORDER BY**—columns used as the basis for sorting the returned data. This parameter is not available for the **Date Histogram** and **Counter** graph types.

- In the drop-down list to the left, select the value that will be used for sorting.
- Select the sort order from the drop-down list on the right: **ASC** for ascending, **DESC** for descending.
- For **Table** type graphs, you can add sorting conditions by clicking **Add column**.

f. **LIMIT** is the maximum number of data points for the widget. This parameter is not available for the **Date Histogram** and **Counter** graph types.

2. Click **Apply**.

Example of search conditions in the query builder



Parameters of search conditions for displaying the average number of bytes per host in the widget

Axes tab

The following table describes the settings on the **Axis** tab.

> The tab is displayed if on the **General tab in the Graph** field you have selected one of the following values: **Bar chart**, **Line chart**, **Date Histogram**.

Description of parameters

Parameter	Description
Point size	Point size on the graph. This field is displayed for the **Line chart** graph type.
Line-width	Width of the line on the graph. This field is displayed for the **Line chart** graph type.
Minimum and maximum values for the Y-axis	Scale of the Y axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Minimum and maximum values for the X-axis	Scale of the X axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Decimals	Number of decimals to which the displayed value must be rounded off.

Appearance tab

The following table describes the settings on the **Appearance** tab.

Description of parameters

Parameter	Description
Description	Description of the widget.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default. Null values are displayed only when the **Show data for previous period** setting is enabled and there is no data for the current period, but there was some data for the previous period.
Color	The color used for displaying the information: • **default** for your browser's default font color • **green** • **red** • **blue** • **yellow** This setting is available for graphs such as **Bar chart**, **Counter**, **Line chart**, **Date Histogram**.
Gradient	Gradient fill of the chart: • Two colors (red and green) • Three colors (red, yellow, and green) This setting is available for charts such as **Bar chart**, **Date Histogram**(with the **Bar chart** type), **Table**. You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold.
Field for gradient indicator	The column in which the gradient fill indicators are displayed. This setting is available for charts of the **Table** type.
Horizontal	Makes the histogram horizontal instead of vertical. When this option is enabled, when a widget displays a large amount of data, horizontal scrolling is not available and all available information is fit into the fixed size of the widget. If there is a lot of data to display, it is recommended to increase the widget size.

Parameter	Description
Show total	Displays the sum total of values. The rounding of the value is determined by the **Decimals** setting. This setting is available for **Pie chart**, **Bar chart**, and **Date Histogram** chart types. The toggle switch is turned off by default.
Period segments length	Duration of the segments into which you want to divide the period. Available for graphs of the **Date Histogram** type.
Scale	Scale for displaying data. Available for a **Stacked bar chart**. The following values are possible: • **Linear** • **Square** • **Logarithm** The default is **Linear**.
Regression	An option for indicating the average value on the chart. The following values are possible: • **Not set**. • **Linear** • **LOESS** (curve with locally estimated scatterplot smoothing). Available for the **Date Histogram** and **Line chart** types.

Actions tab

> This tab is not displayed if you have selected one of the following values on the **General** tab, in the **Graph** field: **Counter**, **Speedometer chart**, **Table**.

Settings on this tab let you configure left-click actions on various elements of widgets, for example, on a chart segment or the text of a legend item. You can select the following actions:

- Go to events.
- Filter by variable.

  The settings are described in the scenario for filtering data in multiple widgets.
- Drill down to another dashboard.

  The settings are described in the scenario for drilling down to another dashboard.

Active lists widget

You can use the **Active lists** widget to get analytics based on SQL queries.

When creating this widget, you must specify the settings described in the tables below.

General tab

The following table lists the settings that must be specified on the **Common** tab.

Description of parameters

Parameter	Description
Name	Name of the widget. When saving a report in Excel format, the name of the widget displayed in the header of the sheet is limited to 31 characters. We recommended keeping this limitation in mind when naming widgets.
Graph	Graph type. The following graph types are available: • **Bar chart**. • **Pie chart**. • **Counter**. • **Table**.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Correlator	The name of the correlator that contains the active list for which you want to receive data.
Active list	The name of the active list for which you want to receive data. The same active list can be used by different correlators. However, a separate entity of the active list is created for each correlator. Therefore, the contents of the active lists used by different correlators differ even if the active lists have the same names and IDs.
SQL query field	This field lets you manually enter a query for filtering and searching active list data. The query structure is similar to that used in event search. When creating a query based on active lists, you must consider the following: • For the FROM function, you must specify the `records` value. • If you want to receive data for fields whose names contain spaces and Cyrillic characters, you must also enclose such names in quotes in the query: • In the SELECT function, enclose aliases in double quotes or backticks: "alias", `another alias`. • In the ORDER BY function, enclose aliases in backticks: `another alias`. • Event field values are enclosed in straight single quotes: WHERE DeviceProduct = 'Microsoft'. • Names of event fields do not need to be enclosed in quotes. • If the name of an active list field begins or ends with spaces, these spaces are not displayed by the widget. The field name must not contain spaces only. • If the values of the active list fields contain trailing or leading spaces, it is recommended to use the LIKE '%field value%' function to search by them. • In your query, you can use service fields: _key (the field with the keys of active list records) and _count (the number of times this record has been added to the active list), as well as custom fields. • The "metric" and "value" aliases in SQL queries cannot be edited for any type of active lists analytics widget, except tables. • If a date and time conversion function is used in an SQL query (for example, fromUnixTimestamp64Milli) and the field being processed does not contain a date and time, an error will be displayed in the widget. To avoid this, use functions that can handle a null value. Example: SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250. • Large values for the LIMIT function may lead to browser errors. • If you select Counter as the graph type, you must specify the method of data processing for the values of the SELECT function: `count`, `max`, `min`, `avg`, `sum`. • In widgets with a chart of the **Table** type, the gradient is drawn based on the values of the field specified in the SQL query (for example, `_count`, `value`, `temp`, or `name`). This field can be selected from the **Field for gradient indicator** drop-down list (if the query contains multiple number or time fields, any one of these can be selected). After this, the cells of the selected column are highlighted with gradient fill markers. If a field is not present in the query, the **Appearance** tab does not display the **Gradient** and **Field for gradient indicator** fields. Special considerations apply when using aliases in SQL functions and SELECT, you can use double quotes and backticks: ", `. If you selected Counter as the graph type, aliases can contain Latin and Cyrillic characters, as well as spaces. When using spaces or Cyrillic, the alias must be enclosed in quotation marks: "An alias with a space", `Another alias`. When displaying data for the previous period, sorting by the count(ID) parameter may not work correctly. It is recommended to sort by the metric parameter. For example, SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250.

You can get the names of the tenants in the widget instead of their IDs.

If you want the names of tenants to be displayed in active list widgets instead of tenant IDs, in correlation rules of the correlator, configure the function for populating the active list with information about the corresponding tenant. The configuration process involves the following steps:

1. Export the list of tenants.
2. Create a dictionary of the **Table** type and import the previously obtained list of tenants into the dictionary.
3. Add a local variable with the **dict** function for mapping the tenant name to tenant ID to the correlation rule.

   Example:

   - Variable: `TenantName`
   - Value: `dict ('<Name of the previously created dictionary with tenants>', TenantID)`
4. Add an action with active lists to the correlation rule. This action will write the value of the previously created variable in the key-value format to the active list using the **Set** function. As the key, specify the field of the active list (for example, `Tenant`), and in the value field, reference the previously created variable (for example, `$TenantName`).

When this rule triggers, the name of the tenant mapped by the **dict** function to the ID from the tenant dictionary is placed in the active list. When creating widgets for active lists, you can get the name of the tenant by referring to the name of the field of the active list (in the example above, `Tenant`).

The method described above can be applied to other event fields with IDs.

Examples of SQL queries for receiving analytics based on active lists:

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  This query returns the key of the active list where the field name is "Event source" and the value of this field is "Johannesburg".
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Query for a pie chart, which returns the number of keys in the active list ('count' aggregation over the '_key' field) and all variants of the Status custom field. The widget displays a pie chart with the total number of records in the active list, divided proportionally by the number of possible values for the Status field.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Query for a table, which returns the values of the Name and Status custom fields, as well as the service field '_count' for those records of the active list in which the value of the Description custom field matches ILIKE '%ftp%'. The widget displays a table with the Status, Name, and Number columns.

Axes tab

The following table lists the settings that must be specified on the **Axis** tab.

This tab is displayed if on the **Common** tab, in the **Graph** field, you have selected **Bar chart**.

Description of parameters

Settings	Description
Min - Max	Scale of the Y axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Min - Max	Scale of the X axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.

Appearance tab

The following table lists the settings that must be specified on the **Appearance** tab.

Description of parameters

Parameter	Description
Description	Description of the widget.
Color	The color used for displaying the information: • **default** for your browser's default font color • **green** • **red** • **blue** • **yellow**
Gradient	Gradient fill of the chart: • Two colors (red and green) • Three colors (red, yellow, and green) The setting is available for **Bar charts** and **Tables**. You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold.
Field for gradient indicator	The column in which the gradient fill indicators are displayed. This setting is available for charts of the **Table** type.
Horizontal	Makes the histogram horizontal instead of vertical. When this setting is enabled, all available information is fitted into the configured widget size. If the amount of data is great, you can increase the size of the widget to display it optimally.
Show total	Displays the sum total of values. The rounding of the value is determined by the **Decimals** setting. This setting is available for **Pie charts** and **Bar charts**. The toggle switch is turned off by default.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default. Null values are displayed only when the **Show data for previous period** setting is enabled and there is no data for the current period, but there was some data for the previous period.

Context tables widget

You can use the **Context tables** widget to get analytics based on SQL queries.

When creating this widget, you must specify the settings described in the tables below.

General tab

The following table lists the settings that must be specified on the **Common** tab.

Description of parameters

Parameter	Description
Name	Name of the widget. When saving a report in Excel format, the name of the widget displayed in the header of the sheet is limited to 31 characters. We recommended keeping this limitation in mind when naming widgets.
Graph	Graph type. The following graph types are available: • **Bar chart**. • **Pie chart**. • **Counter**. • **Table**.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Correlator	Name of the correlator that contains the context table for which you want to receive information.
Context table	Name of the context table for which you want to receive information. The same context table can be used in multiple correlators. However, a separate entity of the context table is created for each correlator. Therefore, the contents of the context tables used by different correlators are different even if the context tables have the same name and ID.

SQL query field	This field lets you manually enter a query for filtering and searching context table data. By default, for each widget type, the field contains a query that obtains the context table schema and the key by key fields.
	The query structure is similar to that used in event search.
	When creating a query based on context tables, you must consider the following:
	• For the `FROM` function, you must specify the `` `records` `` value.
	• You can get data only for the fields specified in the context table schema.
	• You can use supported features of ClickHouse.
	• If you want to receive data for fields whose names contain spaces and Cyrillic characters, you must also enclose such names in quotes in the query:
	  • In the `SELECT` function, enclose aliases in double quotes or backticks: `"< alias >"`, `` `< another alias >` ``.
	  • In the `ORDER BY` function, enclose aliases in backticks: `` `< another alias >` ``.
	  • Event field values are enclosed in straight single quotes: `WHERE DeviceProduct = 'Microsoft'`.
	• Names of event fields do not need to be enclosed in quotes.
	• If the name of an active list field begins or ends with spaces, these spaces are not displayed by the widget. The field name must not contain spaces only.
	• If the values of the active list fields contain trailing or leading spaces, it is recommended to use the `LIKE '%< field value >%'` function to search by them.
	• You can use the `_count` service field (how many times this record has been added to the context table), as well as custom fields.
	• The `metric` and `value` aliases in SQL queries cannot be edited for any type of active lists analytics widget, except tables.
	• If a date and time conversion function is used in an SQL query (for example, `fromUnixTimestamp64Milli`) and the field being processed does not contain a date and time, an error will be displayed in the widget. To avoid this, use functions that can handle a null value. Example: `SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM` `` `records` `` `LIMIT 250`.
	• Large values for the `LIMIT` function may lead to browser errors.
	• If you select **Counter** as the chart type, you must specify the method of data processing for the values of the `SELECT` function: `count`, `max`, `min`, `avg`, `sum`.
	• In widgets with a chart of the **Table** type, the gradient is available only for fields of the **INT** and **FLOAT** types and for the **_count** field. You can select the field in the **Field for gradient indicator** drop-down list. After this, the cells of the selected column are highlighted with gradient fill markers.
	Special considerations when using aliases in SQL functions and `SELECT` statements: you may use double quotes and backticks: `"`, `` ` ``.
	When using spaces or non-Latin characters, the alias must be enclosed in double quotes: `"< Alias with a space >"`, values must be enclosed in straight single quotes: `'< Value with a space >'`.
	When displaying data for the previous period, sorting by the `count(ID)` parameter may not work correctly. We recommend sorting by the `metric` parameter. For example, `SELECT count(ID) AS "metric", Name AS "value" FROM` `` `events` `` `GROUP BY Name ORDER BY metric ASC LIMIT 250`.

You can get the names of the tenants in the widget instead of their IDs.

If you want the names of tenants to be displayed in active list widgets instead of tenant IDs, in correlation rules of the correlator, configure the function for populating the active list with information about the corresponding tenant. The configuration process involves the following steps:

1. Export the list of tenants.
2. Create a dictionary of the **Table** type and import the previously obtained list of tenants into the dictionary.
3. Add a local variable with the **dict** function for mapping the tenant name to tenant ID to the correlation rule.

   Example:

   - Variable: `TenantName`
   - Value: `dict ('<Name of the previously created dictionary with tenants>', TenantID)`
4. Add an action with active lists to the correlation rule. This action will write the value of the previously created variable in the key-value format to the active list using the **Set** function. As the key, specify the field of the active list (for example, `Tenant`), and in the value field, reference the previously created variable (for example, `$TenantName`).

When this rule triggers, the name of the tenant mapped by the **dict** function to the ID from the tenant dictionary is placed in the active list. When creating widgets for active lists, you can get the name of the tenant by referring to the name of the field of the active list (in the example above, `Tenant`).

The method described above can be applied to other event fields with IDs.

Examples of SQL queries for receiving analytics based on active lists:

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  This query returns the key of the active list where the field name is `"Event source"` and the value of this field is `"Johannesburg"`.
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Query for a pie chart, which returns the number of keys in the active list (`count` aggregation over the `_key` field) and all variants of the `Status` custom field. The widget displays a pie chart with the total number of records in the active list, divided proportionally by the number of possible values for the `Status` field.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Query for a table, which returns the values of the `Name` and `Status` custom fields, as well as the service field `_count` for those records of the active list in which the value of the `Description` custom field matches `ILIKE '%ftp%'`. The widget displays a table with the `Status`, `Name`, and `Number` columns.

Axes tab

The following table lists the settings that must be specified on the **Axis** tab.

This tab is displayed if on the **Common** tab, in the **Graph** field, you have selected **Bar chart**.

Description of parameters

Parameter	Description
Min - Max	Scale of the Y axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Min - Max	Scale of the X axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.

Appearance tab

The following table lists the settings that must be specified on the **Appearance** tab.

Description of parameters

Settings	Description
Description	Description of the widget.
Color	The color used for displaying the information: • **default** for your browser's default font color • **green** • **red** • **blue** • **yellow**
Gradient	Gradient fill of the chart: • Two colors (red and green) • Three colors (red, yellow, and green) The setting is available for **Bar charts** and **Tables**. You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold.
Field for gradient indicator	The column in which the gradient fill indicators are displayed. This setting is available for charts of the **Table** type.
Horizontal	Makes the histogram horizontal instead of vertical. When this setting is enabled, all available information is fitted into the configured widget size. If the amount of data is great, you can increase the size of the widget to display it optimally.
Show total	Displays the sum total of values. The rounding of the value is determined by the **Decimals** setting. This setting is available for **Pie charts** and **Bar charts**. The toggle switch is turned off by default.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default. Null values are displayed only when the **Show data for previous period** setting is enabled and there is no data for the current period, but there was some data for the previous period.

Assets customized widget

You can use the **Assets** → **Customized widget** to get advanced asset analytics from processed events using the query builder. In the query, you must specify the asset field and the corresponding condition or set of conditions by which you want the assets to be counted (Y-axis). You can also specify one or more additional conditions (categories) to be used for comparing the number of assets for each field.

When creating the custom widget for assets, you must specify the settings described in the tables below.

General tab

The following table describes the settings on the **General** tab.

Description of parameters

Parameter	Description
Name	Name of the widget. When saving a report in Excel format, the name of the widget displayed in the header of the sheet is limited to 31 characters. We recommended keeping this limitation in mind when naming widgets.
Graph	Graph type. The following graph types are available: • **Pie chart**. The distribution of assets by the specified categories is displayed for all selected tenants. • **Counter**. Assets are counted based on a single condition. The chart displays the sum of assets that match the condition across all selected tenants. • **Table**. Assets are counted by the specified categories across all selected tenants. Each category in the chart has a corresponding row. The category name is displayed in the **value** column. The number of assets matching the condition is displayed in the **metric** column. • **Stacked bar chart** Assets are counted by the specified categories across all selected tenants, and you can group assets by tenants (in this case, individual tenants are arranged along the X axis). Each category has its own zone on the bars of the chart, represented by its own color. Category names are displayed in the legend. You can use check boxes to the left of category names to hide or show the corresponding areas on the bars. • **Speedometer chart** Displays the ratio of the number of assets that match the specified criteria to the total number of assets. The values on the graph are indicated as percentages.
Format	The setting is available for a **Stacked bar chart**. Data display format: **Absolute values** or **Relative values, %**. If you select the **Absolute values** format, the heights of the bars correspond to the sum of the values of the measured indicator. If you select the **Relative values, %** format, all bars have the same height of 100%, and the relative heights of colored zones on the bars correspond to the ratios of indicator values. By default, **Absolute values** is selected.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Asset category	The asset category for which the widget is displaying data.
Search in uncategorized assets	This setting lets you display assets that do not have a category. This check box is cleared by default.
Selecting Graphic Axes group of settings	
Y-axis	Required setting. Asset field and the condition or set of conditions specified for this field, that define how assets are to be counted.
Y axis category	Category for the selected field. Not used for a graph of the **Counter** type. This setting is optional for Y-axis fields whose values are enumerations (can be selected from a finite list of values). For all other fields, this parameter is required.
Group by tenant	The setting is available for a **Stacked bar chart**. Enables additional grouping of assets by tenant. If the check box is selected, assets on the chart are broken up along the X-axis into bars corresponding to individual tenants. If the check box is cleared, all assets are displayed on the same bar. This check box is cleared by default.

Appearance tab.

The following table describes the settings on the **Appearance** tab.

Description of parameters

Parameter	Description
Description	Description of the widget.
Show total	This setting is available for charts of the **Pie chart** type. Enables the display of totals in the chart, in addition to the selected categories. If this check box is enabled, the sum of the values of all specified categories is displayed in the center of the pie chart and in the legend in a separate **Total** column. The toggle switch is turned off by default.
Color	This setting is available for charts of the **Counter** type. The color used for displaying the information: • **default** for your browser's default font color • **green** • **red** • **blue** • **yellow**
Gradient	Gradient fill of the chart: • Two colors (red and green) • three colors (red, yellow, and green) This setting is available for charts of the **Table** type. You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold.
Field for gradient indicator	The column in which the gradient fill indicators are displayed. This column is determined by the **Metric** field selected in the drop-down list. This setting is available for charts of the **Table** type.
Horizontal	Makes the histogram horizontal instead of vertical. When this option is enabled, when a widget displays a large amount of data, horizontal scrolling is not available and all available information is fit into the fixed size of the widget. If there is a lot of data to display, it is recommended to increase the widget size.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default. Null values are displayed only when the **Show data for previous period** setting is enabled and there is no data for the current period, but there was some data for the previous period.
Show percentages in legend	Displays percentage values in the legend. The toggle switch is enabled by default.
Decimals	Number of decimals to which the displayed value must be rounded off.
Scale	Available for a **Stacked bar chart**. Scale for displaying data. The following values are possible: • **Linear** • **Square** • **Logarithm** The default is **Linear**.
Threshold	Available for a **Speedometer chart**. By default, the following ranges are specified: 0–30, 30–70, 70–100.

Image widget

This widget allows adding an image to a dashboard or a report. For example, you can use the **Image** widget to brand a dashboard or report with your company logo.

The **Image** widget does not have a sidebar with settings.

To add an image file, hover over the widget and click **Upload image**; in the file selection window, select a file, and after adding the file to the widget, click **Save**.

You can add multiple **Image** widgets to your dashboard. You can move the widgets around your dashboard and rearrange them by dragging the (⠿) button.

You can create a dashboard with an **Image** widget without adding an image file, for example, to design a layout. KUMA will save the dashboard, and you can edit it later by clicking the **Edit** button on the toolbar, and add an image.

Minimum widget dimensions: 225x161 pixels. Maximum dimensions: 465x692 pixels. You can click the (⤡) button to resize the image in the widget. When resizing, the image is not cropped, but scaled relative to the size of the widget.

Maximum image file size: 3 MB.

Supported image file formats: xbm, tif, pjp, apng, svgz, jpg, jpeg, heif, ico, tiff, webp, jfif, heic, gif, svg, png, bmp, pjpeg, avif.

Downloading widget details in CSV format is not supported.

You can create, edit, duplicate, or delete this widget.

Text widget

This widget allows adding arbitrary text to a dashboard or a report. For example, you can use the **Text** widget to display a title or a brief description of the dashboard or report.

To add or edit text, click on the widget. This activates a text box, and a panel appears that allows formatting the text. You can enter up to 2000 characters.

The **Text** widget does not have a sidebar with settings. A widget of this type cannot be downloaded in CSV format.

Other widgets

This section describes the settings for all widgets, except for the Events, Active lists, Context tables, and Custom Asset widget.

The set of parameters available for a widget depends on the type of graph that is displayed on the widget. The following graph types are available in KUMA:

- Pie chart (◔).
- Counter (4).
- Table (▦).
- Bar chart (≡).
- Date Histogram (📊).
- Line chart
- Stacked Bar chart
- Speedometer chart.

Settings for pie charts

The following table below lists the settings of a **Pie chart**.

Description of parameters

Parameter	Description
Name	Name of the widget. When saving a report in Excel format, the name of the widget displayed in the header of the sheet is limited to 31 characters. We recommended keeping this limitation in mind when naming widgets.
Description	Description of the widget.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Time interval	Period for which data is displayed in the widget. The default is **As layout**, meaning that data is displayed for the period selected for the layout. You can also specify a period for the widget in one of the following ways: • Select the exact start and end date and time of the period in the calendar and click **Apply**. • Select a period relative to the present time in the **Relative period** list. • Specify a value manually: select an exact date and time or a relative period, or a combination of both. For details, see the *Configuring a period* subsection below.
Show total	Displays the sum total of values. The rounding of the value is determined by the **Decimals** setting. The toggle switch is turned off by default.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default.
Decimals	Number of decimals to which the displayed value must be rounded off.

Settings for counters

The following table below lists the settings of a **Counter**.

Description of parameters

Parameter	Description
Name	Name of the widget.
Description	Description of the widget.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Time interval	Period for which data is displayed in the widget. The default is **As layout**, meaning that data is displayed for the period selected for the layout. You can also specify a period for the widget in one of the following ways: • Select the exact start and end date and time of the period in the calendar and click **Apply**. • Select a period relative to the present time in the **Relative period** list. • Specify a value manually: select an exact date and time or a relative period, or a combination of both. For details, see the *Configuring a period* subsection below.

Settings for tables

The following table below lists the settings of a **Table**.

Description of parameters

Parameter	Description
Name	Name of the widget.
Description	Description of the widget.

Parameter	Description
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Time interval	Period for which data is displayed in the widget. The default is **As layout**, meaning that data is displayed for the period selected for the layout. You can also specify a period for the widget in one of the following ways: • Select the exact start and end date and time of the period in the calendar and click **Apply**. • Select a period relative to the present time in the **Relative period** list. • Specify a value manually: select an exact date and time or a relative period, or a combination of both. For details, see the *Configuring a period* subsection below.
Gradient	Gradient fill of the chart: • Two colors (red and green) • Three colors (red, yellow, and green) You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold.
Field for gradient indicator	The column in which the gradient fill indicators are displayed. This column is determined by the field selected in the drop-down list. The type of the field depends on the type of the widget: • For **Affected assets**, it is the **Frequency** field. • For **Affected assets in incidents**, **Real-time protection extended status of KSC assets**, **Affected users in incidents**, it is the **Count** field.
Decimals	Number of decimals to which the displayed value must be rounded off.

Settings for Bar charts, Stacked bar charts, and Date Histograms

The table below lists the settings for the **Bar chart** and **Date Histogram** type graphs located on the **Axis** tab.

Description of parameters

Parameter	Description
Min - Max	Scale of the Y axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Min - Max	Scale of the X axis. Negative values can be displayed on chart axes. This is due to the scaling of charts on the widget and can be fixed by setting zero as the minimum chart values instead of **Auto**.
Decimals	Number of decimals to which the displayed value must be rounded off.

The table below lists the settings for the **Bar chart**, **Stacked bar chart**, and **Date Histogram** type graphs located on the **Appearance** tab.

Description of parameters

Parameter	Description
Name	Name of the widget.
Description	Description of the widget.
Tenant	The tenant for which data is displayed in the widget. You can select multiple tenants. By default, data is displayed for tenants selected in layout settings.
Time interval	Period for which data is displayed in the widget. The default is **As layout**, meaning that data is displayed for the period selected for the layout. You can also specify a period for the widget in one of the following ways: • Select the exact start and end date and time of the period in the calendar and click **Apply**. • Select a period relative to the present time in the **Relative period** list. • Specify a value manually: select an exact date and time or a relative period, or a combination of both. For details, see the *Configuring a period* subsection below.

Parameter	Description
Format	Data display format: **Absolute values** or **Relative values, %**. The setting is available for a **Stacked bar chart**. If you select the **Absolute values** format, the heights of the bars correspond to the sum of the values of the measured indicator. If you select the **Relative values, %** format, all bars have the same height of 100%, and the relative heights of colored zones on the bars correspond to the ratios of indicator values. By default, **Absolute values** is selected.
Timeline view	Time data display format: **Bar chart** or **Line chart**. This setting is available for charts of the **Date Histogram** type. When you select the **Bar chart** format, the data is displayed as vertical bars by default. If the SQL query contains an additional field with the `category` alias, the chart becomes a stacked bar chart, that is, each bar is divided into stripes in accordance with the values of this field. When you select the **Line chart** format, the data is displayed as one or more (depending on the query) polylines drawn through points on the time axis. The **Bar chart** format is selected by default.
Show data for previous period	Enable the display of data for two periods at the same time: the current period and the previous period.
Color	The color used for displaying the information: • **default** for your browser's default font color • **green** • **red** • **blue** • **yellow**
Gradient	Gradient fill of the chart: • Two colors (red and green) • Three colors (red, yellow, and green) You can adjust the direction of the fill by clicking the toggle direction icon (⇆); you can also set thresholds. If not set manually, gradient thresholds are calculated automatically from the data. If there is no data between the specified thresholds, the gradient is not applied. Instead, two colors are used: one for values below the lower threshold, and the other for values above the upper threshold. Gradient fill is not applied to stacked bar charts. In this case, colors are assigned automatically.
Horizontal	Makes the histogram horizontal instead of vertical. When this setting is enabled, all available information is fitted into the configured widget size. If the amount of data is great, you can enlarge the widget to better fit the data.
Show total	Displays the sum total of values. The rounding of the value is determined by the **Decimals** setting. The toggle switch is turned off by default.
Show legend	Displays a legend for the analytics. The toggle switch is turned on by default.
Show nulls in legend	Displays parameters with a null value in the legend for analytics. The toggle switch is enabled by default. Null values are displayed only when the **Show data for previous period** setting is enabled and there is no data for the current period, but there was some data for the previous period.
Period segments length	Duration of the segments into which you want to divide the period. Available for graphs of the **Date Histogram** type.

Settings of Speedometer charts

The table below lists the settings of a **Speedometer chart**.

> The values on the graph are indicated as percentages.

Description of parameters

Parameter	Description
General tab	
Name	Name of the widget.
Tenant	The tenant whose data is displayed in the widget. You can only select tenants that you selected earlier in the dashboard settings.
Asset category	Assets of the selected category in which values will be searched.

Parameter	Description
Search in uncategorized assets	When searching for assets for the chart, asset categories are disregarded.
Y-axis	The value of the parameter by which the search for assets and subsequent calculation of the speedometer reading will be performed. You can specify multiple parameter values to search for assets.
Appearance tab	
Description	Description of the chart that is displayed on the widget.
Threshold	To help you visually identify the severity of an event, the dial of the speedometer is divided into three areas: green, yellow, and red. By default, the following intervals are configured for these areas: • Green: 0–30 • Yellow: 30–70 • Red: 70–100 You can change the ranges as necessary.

Configuring a period

For graphs such as **Pie chart**, **Counter**, **Table**, **Bar chart**, **Stacked bar chart**, **Date Histogram**, you can configure the period for displaying data in the widget using the **Period** setting. By default, the data display period of the widget is the same as the data display period of the dashboard.

To configure the data display period, do one of the following:

- If necessary, change the date and time in the **Time period** setting in one of the following ways:
  - If you want to specify an **exact date**, in the calendar, select the start and end date of the period and click **Apply**.

    You can select a date up to and including the current date. The date and time format depends on your browser settings. If the **Range from** or **Range to** field has a value and you have not edited the time value manually, when you select a date in the calendar, the **Range from** field is automatically populated with `00:00:00,000`, and the **Date to** field is populated with `23:59:59,999`. If you have manually deleted the value in the **Range from** or **Range to** field, when you select a date in the calendar, the field is automatically populated with the current time. Once you select a value in one of the fields, the focus switches to the other field. If your **Range to** is earlier than your **Range from**, this earlier value is automatically inserted into the **Range from** field.

  - If you want to specify a **relative period**, select one of the periods available in the **Relative period** list.

    The period is calculated relative to the current time.

  - If you want to specify a **custom period**, set or edit the value of the **Range from** and **Range to** fields manually.

    You can enter an exact date and time in the `DD.MM.YYYY HH:mm:ss.SSS` format for the Russian localization and `YYYY-MM-DD HH:mm:ss.SSS` for the English localization or a period relative to the current time as a formula. You can also combine these methods. If you do not specify milliseconds when entering the exact date, `000` is substituted automatically. If you have edited the time in the **Range from** or **Range to** fields, picking a date in the calendar does not change the time component.

    In the relative period formulas, you can use the `now` parameter for the current date and time and the interval parameterization language: `+` (only in the **Range to** field), `-`, `/` (rounding to the nearest), as well as time units: `y` (year), `M` (month), `w` (week), `d` (day), `h` (hour), `m` (minute), `s` (second). For example, you can specify the period `now-5d` to get data for the last five days, or `now/w` to get data from the beginning of the first day of the current week (00:00:00:000 UTC) to the current time (`now`).

> The **Range from** field is required, and its value cannot exceed the value of the **Range to** field, and also cannot be earlier than 1970-01-01 (if specifying an exact date or a relative period). The **Range to** cannot be earlier than the **Range from**. If you do not specify a value in the **Range to** from field, `now` is specified automatically.

Kaspersky SIEM stores time values in UTC, but in the web interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select **Today** as the data display period, data will be displayed for the period from 03:00:00.000 until now, not from 00:00:00.000 until now.

If you want to take your time zone into account when selecting a relative data display period, such as **Today**, **Yesterday**, **This week**, or **This month**, you need to manually add a time offset in the **Range from** and **Range to** (if a value other than `now` is specified) by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want to display data for **Yesterday**, you need to change **Range from** to `now-1d/d-3h` and **Date to** to `now/d-3h`. If you want to display data for the **Today** period, you only need to change the value in the **Range from** field to `now/d-3h`.

> If you need results up to 23:59:59:999 UTC of yesterday, you can use an SQL query with a filter by Timestamp or specify an exact date and time.

The bounds of the period are inclusive: for example, for the **Today** time range, events are displayed from the beginning (00:00:00:000 UTC) of the current day to the current time (**now**) inclusive, and for the **Yesterday** period, events are displayed from the beginning (00:00:00:000 UTC) of the previous day to 00:00:00:000 UTC of the current day. You can view the date and time of the last data update and the exact period for which the data is displayed by hovering over the period icon in the widget.

If the **Show data for previous period** setting is enabled for the widget, and the widget is displaying data for a relative period, the tooltip also displays the previous period. The previous period is calculated relative to the current period as start and end values of the current period minus the duration of the current period. For example, if data is updated daily and displayed for a month, but only the first 10 days of the month have passed, the previous period is taken to be the last 10 days of the previous month.

- If you want the widget to display data for the period selected for the layout, click the **Reset** button. Changing the displayed period on the layout also changes the period displayed in the widget.

Filtering widget data

KUMA allows you to filter data in widgets of the **Events** type by selecting filtering parameters in the dashboard. You can filter data in the following cases:

- Filtering data on a single widget

  For this type of filtering, you need to specify one or more local variables in the SQL query in widget properties. Variables allow you to modify this SQL query by substituting the data from the widget on the dashboard into the query. The widget filters the data based on the new values of the variables and refreshes the chart. You do not need to manually change the SQL query in the properties of the widget.

  You can apply local variables by clicking the funnel icon (▽) in the widget. This opens a window in which you can select or enter values for local variables.

- Filtering data in multiple widgets within the same dashboard

  For this type of filtering, you need to specify one or more global variables in dashboard properties. Then add global variables to the SQL queries of the widgets to which you want to apply these global variables. When you assign a new value to a global variable, all widgets that use this variable automatically rebuild charts based on the new value.

Global variables are applied by clicking on a segment of the chart or on text from the legend of the chart. KUMA displays a menu with commands that apply the data category of the selected chart segment or plot legend item to a variable.

- Drilling down to another dashboard while passing filtering parameters

  Global variables can be used to pass values to another dashboard. When drilling down from one dashboard to another, KUMA substitutes the selected value of the variable and the selected time period, and the charts on the new dashboard are automatically rebuilt.

  Local variables cannot be used when drilling down to another dashboard.

> We do not recommend setting more than five variables within a dashboard. This can lead to unstable operation of the dashboard.

Filtering data on a single widget

You can filter data in widgets of the **Events** **type by selecting** filtering parameters in the dashboard.

For filtering data on a single widget, you need to specify one or more local variables in the SQL query in widget properties. Variables allow modifying this SQL query by substituting the data from the widget on the dashboard into the query. The widget filters the data based on the new values of the variables and refreshes the chart. You do not need to manually change the SQL query in the properties of the widget.

For example, such a mechanism can be convenient when an employee that does not have the skills to build SQL queries needs to do an event search. In this case, a KUMA analyst can create a dashboard, add widgets, and configure local variables for them. Subsequently, any employee with access to this dashboard will be able to filter data in widgets without editing SQL queries.

> We do not recommend setting more than five variables for one dashboard. This can lead to unstable operation of the dashboard.

Configuring data filtering on a single widget

To configure local variables for data filtering in one widget:

1. In the **Dashboards** section, select a dashboard and click the **Edit** button to enter the dashboard editing mode.
2. Select an existing **Events** widget or click the **Add widget** button and then select the **Events** widget type.
3. In the widget properties window, select the **General** tab.
4. Under **Defined variables**, click **Add**.
5. Enter an arbitrary name for the variable, then specify the value of the variable. Local and global variable names must be unique within a dashboard.

   As the value of the variable, specify `value` or `category`, that is, the field aliases used in the query. If you want to enter the value of this variable manually when filtering data in the widget, leave this field empty.

   For charts of the **Table** type, you can specify the name of the event field as the value of the variable. This lets you filter the data in the table by the selected value of this field. The name of the event field is displayed in the header of the table column.

6. In the **SQL query** field, in the `WHERE` clause, add a function to handle the variables.

```
The syntax for variables with a specific value is as follows:

filter(<event_field_name> = $variable_name)
```

```
The syntax for variables with an arbitrary value to be entered manually is as follows:

filter(<event_field_name> like $variable_name)
```

In this case, when typing manually, you can use the % metacharacter to search for partial text matches. For detailed information, see the ClickHouse documentation.

> You cannot use the SQL builder to add variables to an SQL query.

View a sample SQL query

```
Example SQL query with a local variable

SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name)
GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250
```

This query uses the local variable `$Name`. The value of the `Name` event field is substituted into this variable. You can apply the variable by clicking the funnel icon ( ) on the widget. This opens a window; in that window, you can specify a value for the variable. The widget filters the selection by the selected value of the `Name` field.

Note that if in the SQL query you specify a variable for a field that takes a numeric value, such a value must be converted to a string. You can do this using the `toString` function. Otherwise, the SQL query returns an error.

```
Example

SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like
$SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

In this query, the `SourcePort` event field has a numeric value, therefore it is converted to a string: `toString(SourcePort)`.

7. Save your changes.

Filtering data on a single widget

To apply a local variables to data filtering within a widget:

1. In the **Dashboards** section, select the dashboard that contains the relevant widget. At least one local variable must be set in the properties of this widget.

2. On the widget, click the funnel icon ( ).

3. This opens a window; in that window, select local variables that you want to apply.

4. Save your changes.

The widget rebuilds the chart taking into account the new value of the variable.

Example of data filtering using local variables

Users may specify credentials in scripts. After the password is changed, scripts still contain credentials with the old password. When running such a script, an authentication error will occur. After several unsuccessful attempts, the user account will be blocked. The technical support specialist will unlock the user account. To avoid repeated account lockouts, the technical support specialist needs to quickly get information about the host where failed authentication attempts are occurring. For this purpose, a KUMA analyst can create a dashboard and add widgets that built using local variables. The analyst configures variables for each widget. The technical support team member who does not have the skills to build SQL queries can use widgets to filter data without editing any SQL queries.

The scenario for filtering data using local variables consists of the following steps:

1. **Configuring data filtering by the KUMA analyst**

   To configure local variables for data filtering in one widget:

   1. In the **Dashboards** section, select a dashboard and click the **Edit** button to enter the dashboard editing mode.
   2. Select an existing **Events** widget or click the **Add widget** button and then select the **Events** widget type.
   3. In the widget properties window, select the **General** tab.
   4. Under **Defined variables**, click **Add**.
   5. Enter the name of the variable (`user_name`). Leave the variable value field empty. In this case, you can enter an arbitrary user name that you want to use to filter events.
   6. In the **SQL query** field enter the following query:

      ```
      SELECT TenantID, Timestamp, Name, DestinationHostName, DestinationUserName FROM `events` WHERE
      DeviceEventClassID='4625' AND filter(DestinationUserName like $user_name) LIMIT 250
      ```

      The entered user name will be used instead of the value in the `DestinationUserName` field.

      Since the query uses the `LIKE` operator, when entering values manually you can use the % metacharacter to search for partial text matches. For detailed information, see the ClickHouse documentation.

      > The above SQL query is valid provided that you use the normalizer from the [OOTB] Microsoft Products for KUMA 3 package.

   7. Save your changes.

2. **Filtering data in the widget by the Technical Support team member**

   To apply a local variables to data filtering within a widget:

   1. In the **Dashboard** section, select the dashboard that contains the widget configured at step 1.
   2. On the widget, click the funnel icon ( ).
   3. In the displayed window, in the `user_name` field, enter the name of the user for which you want to view failed authentication events.
   4. Apply the changes.

The widget filters the data in the table by the specified user name. The `DestinationHostName` column lists hosts that have made failed authentication attempts.

Thus, users can get information without access to the search section, and without the skill of writing SQL queries.

Filtering data in multiple widgets

KUMA allows you to filter data in widgets of the **Events** type by selecting filtering parameters in the dashboard.

To filter data in multiple widgets within one dashboard, you need to specify one or more global variables in the properties of the dashboard. Then add global variables to the SQL queries of the widgets to which you want to apply these global variables. When you assign a new value to a global variable, all widgets that use this variable automatically rebuild charts based on the new value.

Global variables are applied by clicking on a segment of the chart or on text from the legend of the chart. KUMA displays a menu with commands that apply the data category of the selected chart segment or plot legend item to a variable.

> We do not recommend setting more than five variables within a dashboard. This can lead to unstable operation of the dashboard.

Configuring data filtering for multiple widgets at the dashboard level

To configure global variables for filtering data at the dashboard level:

1. In the **Dashboards** section, select a dashboard and click the **Edit** button to enter the dashboard editing mode.
2. Click the **Settings** button.
3. This opens a window; in that window, in the **Variables** section, select the **Global variables** tab.
4. Click **Add**.
5. In the new row, enter the name of the variable. Local and global variable names must be unique within a dashboard.

   The names of all dashboard widgets to which you add global variables are listed in the **Used in widgets** column.

   The names of the global variables are displayed in the commands of the context menu when you click a segment of the chart or an item in the legend of the chart.
6. Save your changes.
7. Select an existing **Events** widget or click the **Add widget** button and then select the **Events** widget type. In this widget, you will be configuring actions on click.
8. In the widget properties window, select the **General** tab.
9. In the **Defined variables** section, add one or more global variables that you have added in the dashboard properties.
10. If necessary, in the SQL query field, add global variables to the WHERE clause using the filter() function. This also applies the configured actions to this widget.

11. Select the **Actions** tab.

    If you want to display a menu with a command to filter data by the selected segment category when a segment of the chart is clicked:

    a. In the **Chart segment** section, enable the **Filter by variable** option.

    b. In the **Category** list, select the variable into which you want to substitute the value of the `category` alias specified in the SQL query.

    The **Category** option is available only for the stacked bar chart type.

    c. In the **Value** list, select the variable into which you want to substitute the value of the `value` alias specified in the SQL query.

    If you want to display a menu with a command to filter data by the selected value when a legend item is clicked:

    a. In the **Legend** item section, enable the **Filter by variable** option.

    If necessary, click the **Copy from chart segment settings** button to automatically transfer the selected parameter values from the **Chart segment** group of settings to the **Legend item** group of settings.

    b. In the **Value** list, select the variables in which you want to be able to substitute legend item variables.

12. In the properties of other widgets to which you want to apply global variables:

    - On the **General** tab, in the **Defined variables** section, add one or more global variables.
    - In the SQL query field of the widget, add global variables to the WHERE clause using the filter() function.

Applying data filtering to multiple widgets at the dashboard level

To apply a global variable to filter data between widgets:

1. In the **Dashboards** section, select the dashboard to whose widgets you want to apply the global variable.
2. Find a widget that has actions on click configured. Click a segment of the graph or on the arrow icon (⌄) next to the legend item to open a menu.
3. In the menu, click **Apply category to variable <variable name>** or **Apply value to variable <variable name>**.

   The value of the selected category or legend item is assigned to the variable. Within the current dashboard, all widgets that use this variable rebuild their charts based on the new value of the variable. Such widgets are marked with a funnel icon with a number indicating the number of filters applied (1). A list of applied global variables is displayed in the upper part of the screen. To clear data filtering for a widget, click the funnel icon with the number (1). To clear data filtering for all widgets on the dashboard, click **Reset all** in the upper part of the dashboard.

Drilling down to a related dashboard

KUMA allows filtering data in widgets of the **Events** type in the current dashboard and drill down to another dashboard while keeping the configured filtering parameters and period.

This is achieved using global variables. The global variables must be configured in both dashboards, as well as in the properties of widgets: on the target dashboard, the variable is specified in the SQL query, and in the source dashboard, the variable is specified when managing the **Drill down to another dashboard** setting. When drilling down from one dashboard to another, KUMA automatically substitutes the selected value of the variable and the period, after which the charts in the target dashboard are rebuilt. Both dashboards must be in the same tenant.

Local variables cannot be used when drilling down to another dashboard.

Configuring the target dashboard

To configure the target dashboard:

1. In the KUMA web interface, in the **Dashboards** section, select a dashboard and create a global variable.

   The variable name may contain only English letters and numerals and may not contain spaces.

2. Save your changes.

3. On the dashboard, select an existing **Events** widget or click the **Add widget** button and then select the **Events** widget type.

4. On the **General** tab, specify the previously created variable:

   - Under **Defined variables**

   - In the **SQL query** field For the SQL query to take into account the value of the variable, add the `filter()` function to the `WHERE` clause.

     The syntax for variables with a specific value is as follows:

     `filter(< event_field_name > = $ variable_name )`

     The syntax for variables with an arbitrary value entered manually is as follows:

     `filter(< event_field_name > like $ variable_name )`

     Query example

     Query with a `$ServiceName` variable:

     ```
     SELECT DestinationHostName AS Host, Name AS Status, Message AS Reason, ServiceName,
     Timestamp AS Time
     FROM events
     WHERE DeviceEventClassID = 'KLSRV_HOST_STATUS_CRITICAL' OR DeviceEventClassID =
     'KLSRV_HOST_STATUS_WARNING' AND filter(ServiceName = $ServiceName)
     ORDER BY Time DESC
     LIMIT 25
     ```

     If a value is passed in the `$ServiceName` variable when drilling down to the target dashboard, the value is automatically substituted into the query and the data is filtered. If the value of the variable is not specified, the query is executed as if the variable was not present.

5. Save your changes.

Configuring the source dashboard

To configure the source dashboard:

1. In the KUMA web interface, in the **Dashboards** section, select a dashboard and create a global variable.

   The variable name must be the same as the name of the variable created in the target dashboard. The name may contain only English letters and numerals and may not contain spaces.

2. Save your changes.

3. On the dashboard, select an existing **Events** widget or click the **Add widget** button and then select the **Events** widget type.

4. On the **General** tab, in the **Defined variables** section, specify the previously created variable.

5. On the **Actions** tab, specify the following settings:

   a. In the **Chart segment** or **Legend item** section, enable **Drill down to another dashboard**.

   b. In the **Dashboards** drop-down list, select the target dashboard.

   c. In the **Value** drop-down list, select the variable whose value you want to pass when drilling down to another dashboard. This must be the same variable that you created earlier.

   The selected variable must be specified in the SQL query of the widget on the target dashboard, so that the data on this widget is automatically filtered after the drill-down.

6. Save your changes.

Drilling down from source dashboard to target dashboard

To drill down to the target dashboard:

1. In the KUMA web interface, under **Dashboards**, select the source dashboard.

2. Find the widget for which you have enabled the **Drill down to another dashboard** option. Click the segment or item in the legend of the chart for which this action is configured.

   This opens the target dashboard in a new tab. The period of the original widget is automatically applied to the entire dashboard, and the selected value from the **Value** drop-down list is passed as a variable to widgets of the **Event** type, in which this variable is used in the SQL query through the `filter()` function. The charts in the widgets on the other dashboards are rebuilt with the passed values taken into account.

   > If you change or delete a variable that is specified in the action on the target dashboard to which you are drilling down to, the drill-down is still performed, but the value of the variable is not passed.

Displaying tenant names in Active list type widgets

If you want the names of tenants to be displayed in **Active list** widgets instead of tenant IDs, in correlation rules of the correlator, configure the function for populating the active list with information about the corresponding tenant.

The configuration process involves the following steps:

1. Export the list of tenants.

2. Create a dictionary of the **Table** type.

3. Import the list of tenants obtained at step 1 into the dictionary created at step 2 of these instructions.

4. Add a local variable with the **dict** function for mapping the tenant name to tenant ID to the correlation rule.

Example:

- Variable: `TenantName`
- Value: `dict ('<Name of the previously created dictionary with tenants>', TenantID)`

5. Add a **Set** action to the correlation rule, which writes the value of the previously created variable to the active list in the <key>-<value> format. As the key, specify the field of the active list (for example, `Tenant`), and in the value field, specify the variable (for example, `$TenantName`).

When this rule triggers, the name of the tenant mapped by the **dict** function to the ID in the tenant dictionary is placed in the active list. When creating widgets based on active lists, the widget displays the name of the tenant instead of the tenant ID.

Response

Response rules let you initiate automatic running of Kaspersky Security Center tasks, Threat Response actions for Kaspersky Endpoint Detection and Response, KICS for Networks, KATA, Active Directory, and running a custom script for specific events.

Automatic execution of Kaspersky Security Center tasks, Kaspersky Endpoint Detection and Response tasks, and KICS for Networks, KATA, and Active Directory tasks in accordance with response rules is available when integrated with the relevant programs.

You can configure response rules under **Resources** → **Response**, and then select the created response rule from the drop-down list in the correlator settings. You can also configure response rules directly in the correlator settings.

Response rules for Kaspersky Security Center

You can configure response rules to automatically start tasks of anti-virus scan and updates on Kaspersky Security Center assets.

When creating and editing response rules for Kaspersky Security Center, you need to define values for the following settings.

General tab

General tab

Setting	Description
Name	Required setting. Unique name of the resource. Must contain 1 to 128 Unicode characters.
Tenant	Required setting. The name of the tenant that owns the resource.
Type	Required setting, available if KUMA is integrated with Kaspersky Security Center. Response rule type, **ksctasks**.

Setting	Description
Kaspersky Security Center task	Required setting. Name of the Kaspersky Security Center task to run. Tasks must be created beforehand, and their names must begin with "`KUMA`". For example, `KUMA antivirus check` (not case-sensitive and without quotation marks). You can use KUMA to run the following types of Kaspersky Security Center tasks: • Update • Virus scan
Event field	Required setting. Defines the event field of the asset for which the Kaspersky Security Center task should be started. Possible values: • SourceAssetID • DestinationAssetID • DeviceAssetID
Handlers	The number of handlers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.
Description	Description of the response rule. You can add up to 4,000 Unicode characters.

Setting	Description
Filter	Used to define the conditions for the events to be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter. **Creating a filter in resources** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

To send requests to Kaspersky Security Center, you must ensure that Kaspersky Security Center is available over the UDP protocol.

If a response rule is owned by the Shared tenant, the displayed Kaspersky Security Center tasks that are available for selection are from the Kaspersky Security Center server that the main tenant is connected to.

If a response rule has a selected task that is absent from the Kaspersky Security Center server that the tenant is connected to, the task is not performed for assets of this tenant. This situation could arise when two tenants are using a common correlator, for example.

Services tab

This tab is displayed only when you edit the settings of the created response rule; on this tab, you can link the rule to correlators.

To link a response rule to a correlator, click the **Link to service** button → **Link to correlator**. This opens a window; in that window, select one or more correlators and click **OK**. The response rule is linked to the selected correlators and is applied in accordance with their configuration.

If necessary, you can unlink the response rule from a service. To do this, select the check box next to the relevant correlator, click **Delete**, and confirm the unlinking from the service.

Response rules for a custom script

You can create a script containing commands to be executed on the KUMA server when selected events are detected and configure response rules to automatically run this script. In this case, the solution will run the script when it receives events that match the response rules.

The script file is stored on the server where the correlator service using the response resource is installed: /opt/kaspersky/kuma/correlator/<correlator ID>/scripts. The `kuma` user of this server requires the permissions to run the script.

When creating and editing response rules for a custom script, you need to define values for the following parameters.

General tab

General tab

Setting	Description
Name	Required setting. Unique name of the resource. Must contain 1 to 128 Unicode characters.
Tenant	Required setting. The name of the tenant that owns the resource.
Type	Required setting. Response rule type, **script**.
Timeout	The number of seconds allotted for the script to finish. If this amount of time is exceeded, the script is terminated.

Setting	Description
Script name	Required setting. Name of the script file. If the response resource is attached to the correlator service but there is no script file in the /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts folder, the correlator will not work.
Script arguments	Arguments or event field values that must be passed to the script. If the script includes actions taken on files, you should specify the absolute path to these files. Parameters can be written with quotation marks ("). Event field names are passed in the `{{.EventField}}` format, where `EventField` is the name of the event field which value must be passed to the script. Example: `-n "\"usr\": {{.SourceUserName}}"`
Handlers	The number of handlers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.
Description	Description of the resource. You can add up to 4,000 Unicode characters.

Setting	Description
Filter	Used to define the conditions for the events to be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter. **Creating a filter in resources** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when you edit the settings of the created response rule; on this tab, you can link the rule to correlators.

To link a response rule to a correlator, click the **Link to service** button → **Link to correlator**. This opens a window; in that window, select one or more correlators and click **OK**. The response rule is linked to the selected correlators and is applied in accordance with their configuration.

If necessary, you can unlink the response rule from a service. To do this, select the check box next to the relevant correlator, click **Delete**, and confirm the unlinking from the service.

Response rules for KICS for Networks

You can configure response rules to automatically trigger response actions on KICS for Networks assets. For example, you can change the asset status in KICS for Networks.

When creating and editing response rules for KICS for Networks, you need to define values for the following settings.

General tab

General tab

Setting	Description
Name	Required setting. Unique name of the resource. Must contain 1 to 128 Unicode characters.
Tenant	Required setting. The name of the tenant that owns the resource.
Type	Required setting. Response rule type, **Response via KICS/KATA**.
Event field	Required setting. Specifies the event field for the asset for which response actions must be performed. Possible values: • SourceAssetID • DestinationAssetID • DeviceAssetID
KICS for Networks task	Response action to be performed when data is received that matches the filter. The following types of response actions are available: • **Change asset status to Authorized**. • **Change asset status to Unauthorized**. When a response rule is triggered, KUMA will send KICS for Networks an API request to change the status of the specified device to **Authorized** or **Unauthorized**.
Handlers	The number of handlers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.
Description	Description of the resource. You can add up to 4,000 Unicode characters.

Setting	Description
Filter	Used to define the conditions for the events to be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter. **Creating a filter in resources** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press `Backspace`.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when you edit the settings of the created response rule; on this tab, you can link the rule to correlators.

To link a response rule to a correlator, click the **Link to service** button → **Link to correlator**. This opens a window; in that window, select one or more correlators and click **OK**. The response rule is linked to the selected correlators and is applied in accordance with their configuration.

If necessary, you can unlink the response rule from a service. To do this, select the check box next to the relevant correlator, click **Delete**, and confirm the unlinking from the service.

Response rules for Kaspersky Endpoint Detection and Response

You can configure response rules to automatically trigger response actions on Kaspersky Endpoint Detection and Response assets. For example, you can configure automatic asset network isolation.

When creating and editing response rules for Kaspersky Endpoint Detection and Response, you need to define values for the following settings.

General tab

General tab

Setting	Description
Event field	Required setting. Specifies the event field for the asset for which response actions must be performed. Possible values: • SourceAssetID • DestinationAssetID • DeviceAssetID

Setting	Description

Task type	Response action to be performed when data is received that matches the filter. The following types of response actions are available:
	• Enable network isolation. When selecting this type of response, you need to define values for the following setting:
	  • **Isolation timeout**—the number of hours during which the network isolation of an asset will be active. You can indicate from 1 to 9,999 hours. If necessary, you can **add an exclusion for network isolation**.
	  To add an exclusion for network isolation:
	  a. Click the **Add exclusion** button.
	  b. Select the direction of network traffic that must not be blocked:
	  • Inbound.
	  • Outbound.
	  • Inbound/Outbound.
	  c. In the **Asset IP** field, enter the IP address of the asset whose network traffic must not be blocked.
	  d. If you selected **Inbound** or **Outbound**, specify the connection ports in the **Remote ports** and **Local ports** fields.
	  e. If you want to add more than one exclusion, click **Add exclusion** and repeat the steps to fill in the **Traffic direction**, **Asset IP**, **Remote ports** and **Local ports** fields.
	  f. If you want to delete an exclusion, click the **Delete** button under the relevant exclusion.
	  When adding exclusions to a network isolation rule, Kaspersky Endpoint Detection and Response may incorrectly display the port values in the rule details. This does not affect application performance. For more details on viewing a network isolation rule, please refer to the *Kaspersky Anti Targeted Attack Platform Help Guide*.
	• Disable network isolation.
	• Add prevention rule. When selecting this type of response, you need to define values for the following settings:
	  • **Event fields to extract hash from**—event fields from which KUMA extracts SHA256 or MD5 hashes of files that must be prevented from running.
	  The selected event fields, as well as the values selected in the **Event field**, must be added to the propagated fields of the correlation rule.
	  • **File hash #1**—SHA256 or MD5 hash of the file to be blocked.
	  At least one of the above fields must be completed.
	• Delete prevention rule.
	• Run program. When selecting this type of response, you need to define values for the following settings:
	  • **File path**—path to the file of the process that you want to start.
	  • **Command line parameters**—parameters with which you want to start the file.
	  • **Working directory**—directory in which the file is located at the time of startup.
	  When a response rule is triggered for users with the General Administrator role, the **Run program** task will be displayed in the **Task manager** section of the solution web interface. In the **Created by** column of the task table, **Scheduled task** is displayed for this task. You can view task completion results.
	  All of the listed operations can be performed on assets that have Kaspersky Endpoint Agent for Windows. On assets that have Kaspersky Endpoint Agent for Linux, the application can only be started.
	  At the software level, the capability to create prevention rules and network isolation rules for assets with Kaspersky Endpoint Agent for Linux is unlimited. KUMA and Kaspersky Endpoint Detection and Response do not provide any notifications about unsuccessful application of these rules.

Handlers	The number of handlers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.
Description	Description of the response rule. You can add up to 4,000 Unicode characters.

Setting	Description
Filter	Used to define the conditions for the events to be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter. **Creating a filter in resources** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⣿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when you edit the settings of the created response rule; on this tab, you can link the rule to correlators.

To link a response rule to a correlator, click the **Link to service** button → **Link to correlator**. This opens a window; in that window, select one or more correlators and click **OK**. The response rule is linked to the selected correlators and is applied in accordance with their configuration.

If necessary, you can unlink the response rule from a service. To do this, select the check box next to the relevant correlator, click **Delete**, and confirm the unlinking from the service.

Active Directory response rules

Active Directory response rules define the actions to be applied to an account if a rule is triggered.

When creating and editing response rules using Active Directory, specify the values for the following settings.

General tab

General tab

Setting	Description
Name	Required setting. Unique name of the resource. Must contain 1 to 128 Unicode characters.
Tenant	Required setting. The name of the tenant that owns the resource.
Type	Required setting. Response rule type, **Response via Active Directory**.
Source of the user account ID	Event field from which the Active Directory account ID value is taken. Possible values: • SourceAccountID • DestinationAccountID

Setting	Description
AD command	Command that is applied to the account when the response rule is triggered. Available values: • **Add account to group** The Active Directory group to move the account from or to. In the mandatory field **Distinguished name**, you must specify the full path to the group. For example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com. Only one group can be specified within one operation. • **Remove account from group** The Active Directory group to move the account from or to. In the mandatory field **Distinguished name**, you must specify the full path to the group. For example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com. Only one group can be specified within one operation. • Reset account password If your Active Directory domain allows selecting the **User cannot change password** check box, resetting the user account password as a response will result in a conflict of requirements for the user account: the user will not be able to authenticate. The domain administrator will need to clear one of the check boxes for the affected user account: **User cannot change password** or **User must change password at next logon**. • Block account
Group DN	The DistinguishedName of the domain group in fields for each role. The users of this domain group must be able to authenticate with their domain user accounts. Example of entering a group: OU=KUMA users,OU=users,DC=example,DC=domain
Handlers	The number of handlers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.

Setting	Description
Filter	Used to define the conditions for the events to be processed using the response rule. You can select an existing filter from the drop-down list or **create** a new filter. **Creating a filter in resources** All fields of a KUMA event have a default value. For all numeric fields, the default value is `0`. For all string fields, the default value is an empty string. An event not having a field means the field has the default value. Therefore, an event can trigger a filter even if the event does not have the field specified in the filter. For example, if you specify a `DestinationPort <= 1024` condition in the filter, but the event does not contain the `DestinationPort` field, the filter is triggered anyway because `DestinationPort = 0` by default. *To create a filter:* 1. In the **Filter** drop-down list, select **Create new**. 2. To save the filter and use it for other resources, select the **Save filter** check box. This check box is cleared by default. 3. If you selected the **Save filter** check box, enter a name for the new filter in the **Name** field. Maximum length of the name: 128 Unicode characters. 4. Select the filter creation mode: **Constructor** or **Code**. When creating filtering conditions, you can switch between modes. In this case, the generated filter conditions are saved. If the filter code is not displayed on the **Code** tab after linking the created filter to the resource, go to the **Builder** tab and then go back to the **Code** tab to display the filter code. 5. If you selected the **Constructor** option, do the following: a. In the drop-down list select a boolean operator: • **AND**: selects events that match all of the specified conditions. • **OR**: selects events that match one of the specified conditions. • **NOT**: selects events that match none of the specified conditions. b. Click the **Add condition** button. c. If you want to add a negative condition, from the **If** drop-down list, select **If not**. d. From the drop-down lists, select operands and filter operators. **Operands of filters** • **Event fields** specify the field of the event that you need to use as a filter operand. • **Active lists** specify the active list or field of the active list that you need to use as a filter operand. When selecting an active list, specify one or more event fields that are used to create an active list entry and act as a key of an active list entry. To finish specifying event fields, press **`Ctrl`**/**`Command`**+**`F1`**. If you have not specified the **inActiveList** operator, you need to specify the name of the active list field that you want to use as a filter operand. • **Dictionaries** is a value from the dictionary resource that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the dictionary that you want to use. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • In the **Context tables** section, you can specify the value of the context table that you want to use as the filter operand. When selecting a context table, you must specify an event field: • **context table name** (required) is the context table that you want to use. • **key fields** (required) are event fields or local variables that are used to create a context table record and serve as the key for the context table record. • **field** is the name of the context table field from which you want to get the value of the operand. • **index** is the index of the list field of the table from which you want to get the value of the operand. • **Tables** specifies user-defined values that you need to assign to the operand. Advanced settings: • **dictionary** (required) is the type of the dictionary. You need to select the **Table** dictionary type. • **key fields** (required) are event fields that are used to generate the key of the dictionary value. • **TI** specifies the settings for reading Kaspersky CyberTrace threat intelligence (TI) data from events. Advanced settings: • **stream** (required) is the Kaspersky CyberTrace threat category. • **key fields** (required) is the event field with Kaspersky CyberTrace threat indicators. • **field** (required) is the field of the Kaspersky CyberTrace feed with threat indicators.

Setting	Description

	• **Constant** is a user-defined value that you want to assign to the operand. Advanced settings:
	  • **value** (required) is the constant that you want to assign to the operand.
	• **List** specifies user-defined values that you want to assign to the operand. Advanced settings:
	  • **value** (required) are the constants that you want to assign to the operand. When you type the value in the field and press **ENTER**, the value is added to the list and you can enter a new value.
	Filter operators
	• **=** means the left operand equals the right operand.
	• **<** means the left operand is less than the right operand.
	• **<=** means the left operand is less than or equal to the right operand.
	• **>** means the left operand is greater than the right operand.
	• **>=** means the left operand is greater than or equal to the right operand.
	• **inSubnet** means the left operand (IP address) is in the subnet of the right operand (subnet).
	• **contains** means the left operand contains values of the right operand.
	• **startsWith** means the left operand starts with one of the values of the right operand.
	• **endsWith** means the left operand ends with one of the values of the right operand.
	• **match** means the left operand matches the regular expression of the right operand. The RE2 regular expressions are used.
	• **hasBit** checks whether the left operand (string or number) contains bits whose positions are listed in the right operand (in a constant or in a list).
	The value to be checked is converted to binary and processed right to left. Chars are checked whose index is specified as a constant or a list.
	If the value being checked is a string, then an attempt is made to convert it to integer and process it in the way described above. If the string cannot be converted to a number, the filter returns `False`.
	• **hasVulnerability** checks whether the left operand contains an asset with the vulnerability and vulnerability severity specified in the right operand.
	If an ID and severity of the vulnerability are not specified, the filter is triggered if the asset in the event being checked has any vulnerability.
	• The **inActiveList** operator has only one operand. Its values are selected in the **Key fields** field and are compared with the entries in the active list selected from the Active List drop-down list.
	• **inDictionary** checks whether the specified dictionary contains an entry defined by the key composed with the concatenated values of the selected event fields.
	• **inCategory** means the asset in the left operand is assigned at least one of the asset categories of the right operand.
	• **inActiveDirectoryGroup** means the Active Directory account in the left operand belongs to one of the Active Directory groups in the right operand.
	• **TIDetect** operator is used to find events using Kaspersky CyberTrace data. This operator can be used only with events that were enriched with data from Kaspersky CyberTrace. In other words, it can only be used in collectors at the destination selection stage and in correlators.
	• **inContextTable** checks for the presence of the entry in the specified context table.
	• **intersect** checks for the presence in the left operand of the list items specified in the right operand.
	If you want the operator to be case-insensitive, select the **do not match case** check box. The action does not apply to the **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit**, and **inDictionary** operators. This check box is cleared by default.
	You can change or delete the specified operator. To change the operator, click it and specify a new operator. To delete the operator, click it, then press **Backspace**.
	e. To add a group of conditions for the filter, click the **Add group** button.
	You can add multiple condition groups.
	6. If you selected the **Code** option, specify the text filter command.
	In the right part of the builder, you can find the navigator, which lets you to navigate the filter code. Line wrapping is performed automatically at **AND**, **OR**, **NOT** logical operators, or at commas that separate the items in the list of values.
	7. To change the order of filter conditions, use the reorder icons ⠿. To remove a condition, click the delete icon ✕.
	8. Click **Save**.

Services tab

This tab is displayed only when you edit the settings of the created response rule; on this tab, you can link the rule to correlators.

To link a response rule to a correlator, click the **Link to service** button → **Link to correlator**. This opens a window; in that window, select one or more correlators and click **OK**. The response rule is linked to the selected correlators and is applied in accordance with their configuration.

If necessary, you can unlink the response rule from a service. To do this, select the check box next to the relevant correlator, click **Delete**, and confirm the unlinking from the service.

Response rules with EDR actions

Starting with KUMA 3.4.1 and Kaspersky Endpoint Security 12.9 for Windows, EDR actions are supported when responding to threats. When correlation events are received, KUMA performs EDR actions. Performing EDR actions requires first setting up response rules. In the properties of response rules, you need to specify the arguments of scripts that you can download by following this link:

https://box.kaspersky.com/d/579c0271a38e440b9144/

When a response rule is triggered, Kaspersky Endpoint Security performs EDR actions and creates the following tasks in Kaspersky Security Center:

- onDemandScan.py performs a Critical Areas Scan.
- ioCScan.py searches for indicators of compromise.
- quarantineFile.py quarantines a file.
- deleteFile.py deletes a file.
- getFile.py gets a file.
- isolateHost.py isolates the computer from the network.
- preventExecution.py prevents execution of objects.

  To perform this task, it is important to make sure that in Kaspersky Security Center, in the **Assets (Devices)** → **Policies & profiles** → <Kaspersky Endpoint Security policy name> → **Application settings** → **Detection and Response** → **Endpoint Detection and Response**, the **Execution Prevention DISABLED** toggle switch is turned off.
- startProcess.py starts a process.
- terminateProcess.py terminates a process

When setting up response rules with EDR actions, we recommend taking into account the load on the computer when running tasks. If the response rules cause scripts to create too many tasks, the computer's performance may be degraded. If there are too many requests, the requests are rotated regardless of whether a particular request has been completed. Kaspersky Endpoint Security allows creating no more than 100 tasks. When this limit is reached, Kaspersky Endpoint Security rotates tasks in Kaspersky Security Center. The lifespan of a task is 30 days.

> Tasks created when the response rules from KUMA are executed are displayed in Kaspersky Endpoint Security of the host on which the response rule is triggered. These tasks are not displayed in Kaspersky Security Center.

You can use reports to view information about the execution of EDR actions in the Administration Console of Kaspersky Security Center. Kaspersky Endpoint Security generates events with descriptions in the '[Response] [kuma] $<script name> - $<date>' format. A description in this format allows creating event selections for EDR actions.

Prerequisites

Before configuring response rules with EDR actions, make sure that the following conditions are satisfied:

1. Integration with Kaspersky Security Center is configured.
2. A separate user has been created in Kaspersky Security Center that has the rights to run all Kaspersky Endpoint Security tasks and tasks that you plan to run using scripts.
3. Integration with Kaspersky Endpoint Security for Windows is configured. When installing Kaspersky Endpoint Security, you must install the EDR component.
4. The following actions have been performed on the host with the correlator:
   a. Python 3.6 or later and the KIAkOAPI Python package are installed.
   b. The scripts have been downloaded from the https://box.kaspersky.com/d/579c0271a38e440b9144/ link and placed in the `/opt/kaspersky/kuma/correlator/<Correlator ID>/scripts` directory.
   c. The scripts are connected to Kaspersky Security Center.

      The credentials are not protected, so we recommend using a separate Kaspersky Security Center user created at step 2 for connecting the scripts to Kaspersky Security Center and restricting access to the directory that contains the scripts. To connect the scripts, open the scripts for editing and edit the lines as follows:

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"
```

Configuring the response

To create a response rule in a KUMA correlator:

1. In the KUMA web interface, in the **Resources and services** → **Correlators** section, create a correlator or open an existing correlator for editing.

2. In the correlator creation wizard, at the **Response** step, click **Add response rule** to open the **Response** window, and in that window, fill in the following fields:

   a. In the **Type** drop-down list, specify the **Run script** response rule type.

   b. In the **Timeout** field, specify the number of seconds allotted for the script to finish. If this value is exceeded, the script is terminated. Set this value to **600** (10 minutes).

   c. In the **Script name** field, enter the name of the script, for example, **deleteFile.py**.

   d. In the **Script arguments** field, specify options or event field values that must be passed to the script. You can use single quotes to specify unescaped characters in options. Arguments of each script are described in expandable boxes.

   onDemandScan.py performs a Critical Areas Scan.

   The onDemandScan script automatically creates and runs the *Critical Areas Scan* task when certain KUMA events are detected. By default, Kaspersky Endpoint Security checks kernel memory, running processes, and boot sectors.

Limitations

If the Kaspersky Sandbox or KATA Sandbox solution is deployed, after updating the management plug-in to version 12.9, you need to re-establish the background connection between Kaspersky Security Center Web Console and the Administration Server. This is necessary to update user rights to the new EDR action functionality for threat responsein KUMA.

Arguments

To configure the *Critical Areas Scan* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--recursive true|false` enables or disables the recursive scanning mode. This argument must be specified manually.

`--path` is a space-delimited list of files and folders for Custom Scan.

You can also select a predefined scan scope. Kaspersky Endpoint Security has the following predefined objects for configuring the scan scope:

- **System memory**.
- **Running processes and Startup Objects**.

  Memory occupied by processes and executable files of applications that run at operating system startup.
- **Disk boot sectors**.

  Boot sectors of hard drives and removable media.
- **System Backup**.

  Contents of the System Volume Information folder.
- **All external devices**.
- **All hard drives**.
- **All network drives**.

To do this, in the onDemandScan script, for the "enabled" setting of the relevant scan scope, set the value to True or False:

```
defaultPreset = [
    {"enabled": False, "path": "%personal%", "recursive": True,
        "type": ScanObjectType.Folder.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.Email.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.SystemMemory.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.StartupObjectsAndRunningProcesses.value},
    {"enabled": True,
     "path": "", "recursive": True, "type": ScanObjectType.DiskBootSectors.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.SystemBackupStorage.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllRemovableDrives.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllFixedDrives.value},
    {"enabled": False,
     "path": "", "recursive": True, "type": ScanObjectType.AllNetworkDrives.value}
```

Example

```
python3 onDemandScan.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --recurive
false --path 'C:\Program Files (x86)\Example Folder'
```

ioCScan.py searches for indicators of compromise.

The iocScan script automatically creates and runs the *IOC Scan* task when certain KUMA events are detected. The *IOC Scan* task allows detecting indicators of compromise on the computer and performing threat response actions.

Kaspersky Endpoint Security uses IOC files to search for indicators of compromise. *IOC files* contain a set of indicators that are matched against events to generate detections. IOC files must conform to the OpenIOC standard.

Limitations

By default, Kaspersky Endpoint Security performs the IOC scan only in critical areas of the computer, such as the Downloads folder, the Desktop, the temporary files folder of the operating system, and others.

By default, the following event logs are selected: Application Event Log, System Event Log, and Security Event Log.

Arguments

To configure the *IOC Scan* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--iocZip` is the path to the ZIP archive with base64-encoded IOC files that you want to use for the scan. Required argument. This argument must be specified manually.

`--isolateHost true|false` specifies whether the computer must be isolated from the network when an indicator of compromise is detected to prevent the spread of the threat. Required argument. This argument must be specified manually.

`--quarantineObject true|false` specifies whether the malicious object must be deleted when an indicator of compromise is detected. Before deleting an object, Kaspersky Endpoint Security creates a backup copy of it in case you need to restore the object later. Kaspersky Endpoint Security then quarantines the backup copy. Required argument. This argument must be specified manually.

`--scanCriticalAreas true|false` specifies whether the *Critical Areas Scan* task must be run when an indicator of compromise is detected. By default, Kaspersky Endpoint Security checks kernel memory, running processes, and boot sectors. Required argument. This argument must be specified manually.

Example

```
python3 iocScan.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --iocZip
'./ioc.zip' --isolateHost true --scanCriticalAreas true --quarantineObject true
```

quarantineFile.py quarantines a file.

The quarantineFile script automatically creates and runs the *Move file to Quarantine* task when certain events are received in KUMA. *Quarantine* is a special local storage on your computer. A user can quarantine files that the user considers dangerous for the computer. Quarantined files are stored in encrypted form and do not pose a threat to the security of the device.

Limitations

The *Move file to Quarantine* task has the following limitations:

1. The file size may not exceed 100 MB.
2. Files required by Kaspersky Endpoint Security for Linux cannot be deleted:
   - Files that are included in the scope of the Kaspersky Endpoint Security for Linux self-defense technology
   - Files digitally signed by Kaspersky

Arguments

To configure the *Move file to Quarantine* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--path` is the path to the file. Required argument. The script gets this argument from the event.

`--md5hash` is the MD5 hash of the file. The script gets this argument from the event.

`--sha256hash` is the SHA256 hash of the file. The script gets this argument from the event.

Examples

```
python3 quarantineFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt'
```

```
python3 quarantineFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --sha256hash 1234567891012345678901234567890 12
```

deleteFile.py deletes a file.

The deleteFile script automatically creates and runs the *Delete file* task when certain KUMA events are detected. For example, you can remotely delete a file when responding to threats.

Limitations

Files required by Kaspersky Endpoint Security for Linux cannot be deleted:

- Files that are included in the scope of the Kaspersky Endpoint Security for Linux self-defense technology
- Files digitally signed by Kaspersky

Arguments

To configure the *Delete file* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--searchInSubfolders true|false` specifies whether subfolders must be traversed in search for the file. Required argument. This argument must be specified manually.

`--path` is the path to the file. Required argument. The script gets this argument from the event.

`--md5hash` is the MD5 hash of the file. The script gets this argument from the event.

`--sha256hash` is the SHA256 hash of the file. The script gets this argument from the event.

Examples

```
python3 deleteFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt' --searchInFolders false
```

```
python3 deleteFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path '1' -
-searchInFolders false --sha256hash 1234567891012345678901234567890 12
```

getFile.py gets a file.

The getFile script automatically creates and runs the *Get file* task when certain events are received in KUMA. For example, you can configure it to fetch an event log file that a third-party application creates. The task saves a copy of the file in the quarantine. *Quarantine* is a special local storage on your computer. You can use the Web Console to download this file to your computer from the quarantine (**Operations** → **Repositories** → **Quarantine**). On the user's computer, the file remains in its original folder.

Limitation

The file size may not exceed 100 MB.

Arguments

To configure the *Get file* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--path` is the path to the file. Required argument. The script gets this argument from the event.

`--md5hash` is the MD5 hash of the file. The script gets this argument from the event.

`--sha256hash` is the SHA256 hash of the file. The script gets this argument from the event.

Examples

```
python3 getFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\File.txt'

python3 getFile.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --md5hash 12345678910123456789012345678901 2
```

isolateHost.py isolates the computer from the network.

The isolateHost script automatically isolates a computer from the network when certain KUMA events are detected.

Once Network Isolation is enabled, the application terminates all active TCP/IP network connections and blocks all new connections on the computer, except for the following connections:

- Connections specified in exclusions from Network Isolation
- Connections initiated by Kaspersky Endpoint Security services
- Connections initiated by the Kaspersky Security Center Network Agent
- Connections to the SVM and Integration Server if the application is being used in Light Agent mode
- Connections to KSN when the application is integrated with Kaspersky Managed Detection and Response

Arguments

To configure Network Isolation, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--action` is the Network Isolation mode. Required argument. This argument must be specified manually. Possible values:

- `1` isolates the computer from the network.
- `0` disables Network Isolation.

Example

```
python3 isolateHost.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --action 1
```

preventExecution.py prevents execution of objects.

The preventExecution script automatically prevents objects from running when certain KUMA events are detected. Execution prevention for objects lets you control the running of executable files and scripts, as well as the opening of office format files. In this way, you can, for example, prevent the launch of applications that you consider unsafe. As a result, the spread of the threat may be stopped. Execution prevention for objects supports a certain set of office file extensions and a certain set of script interpreters. An *execution prevention rule* is a set of criteria that an application takes into account when responding to an object starting, such as when blocking an object from running. The application identifies files by their path or checksum using MD5 and SHA256 hashing algorithms.

> Kaspersky Endpoint Security monitors the creation of new execution prevention rules and ignores duplicate rules. That is, if the launch of an object is already prevented, the application does not create a new rule. For this to be true, all of the parameters of the rule must match (path to the file and file hash), and the rule must be enabled.

Limitations

Execution prevention for objects has the following limitations:

1. Prevention rules do not apply to files on CDs or ISO images. The application does not block the running or opening of such files.
2. A prevention rule cannot be applied to files required by Kaspersky Endpoint Security for Linux:
   - Files that are included in the scope of the Kaspersky Endpoint Security for Linux self-defense technology
   - Files digitally signed by Kaspersky
3. We do not recommended creating more than 5000 execution prevention rules because this may make the system unstable.

Arguments

To configure Execution prevention for objects, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--hash` is the MD5 hash of the file. Required argument. The script gets this argument from the event.

`--path` is the full path to the file, or the path to the file if you enter the file hash. Required argument. The script gets this argument from the event.

Example

```
python3 preventExecution.py --targetHost '422db51e-9383-46d4-b75d-f4d1d20fff2c' --
path 'C:\test5\run10.exe' --hash '8806b7f358884a049675b42c5f75ba10'
```

startProcess.py starts a process.

The startProcess script automatically creates and runs the *Start process* task when certain KUMA events are detected. For example, you can remotely run a utility that creates a report about the computer's configuration. You can then use the *Get file* task to receive the created report file in the Kaspersky Security Center Web Console.

Arguments

To configure the *Start process* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--executablePath` is the path to the file. Required argument. You can pass this argument from the event or enter a value manually.

`--arguments` lists additional command line arguments for the process. These arguments must be specified manually.

`--workingFolder` is the path to the working folder of the process. This argument must be specified manually.

Example

```
python3 startProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --
executablePath 'c://a/a.exe'
```

terminateProcess.py terminates a process.

The terminateProcess script automatically creates and runs the *Terminate process* task when certain KUMA events are detected. For example, you can remotely terminate an internet speed test utility that was launched by the *Run process* task.

If you want to prevent a file from running, you can configure the Execution prevention for objects component. You can prevent the execution of executable files, scripts, office format files.

Limitations

Processes of files required by Kaspersky Endpoint Security for Windows cannot be terminated:

- Files that are included in the scope of the Kaspersky Endpoint Security for Windows self-defense technology
- Files digitally signed by Kaspersky

Arguments

To configure the *Terminate process* task, you need to specify the following arguments for the script:

`--targetHost` is the ID of the computer on which the script must be run. Required argument. The script gets this argument from the event.

`--caseSensitive true|false` enables or disables the case-sensitive mode when searching for the file. Required argument. This argument must be specified manually.

`--path` is the path to the file. Required argument. The script gets this argument from the event.

`--md5hash` is the MD5 hash of the file. The script gets this argument from the event.

`--sha256hash` is the SHA256 hash of the file. The script gets this argument from the event.

Examples

```
python3 terminateProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\file.exe' --caseSensitive true

python3 terminateProcess.py --targetHost 004c7fcd-8940-4d62-8a94-911932dc861b --path
'C:\Folder\' --caseSensitive false --md5hash 12345678910123456789012345678901 2
```

e. In the **Workers** field, specify the number of workers that the service can run simultaneously to process response rules in parallel. By default, the number of handlers is the same as the number of virtual processors on the server where the service is installed.

f. If necessary, enter an arbitrary description of the response rule in the **Description** field.

g. In the **Filter** field, specify conditions that events must satisfy for the response rule to be applied.

3. Save settings and install the correlator service on the server or restart the active correlator to apply the settings.

When a correlation event with certain fields is received, it triggers the response rule in KUMA, which initiates the EDR action. As a result, a corresponding task is created and run in Kaspersky Security Center. You can view the relevant records in Kaspersky Security Center logs and Kaspersky Endpoint Security logs.

Working with events

Events are information security events registered on the monitored elements of the corporate IT infrastructure. For example, events include login attempts, interactions with a database, and information sent by sensors. Each individual event may appear meaningless, but taken together, they paint a bigger picture of network activity that can help you identify security threats. This is the core functionality of KUMA.

KUMA receives events from logs and restructures them by bringing data from heterogeneous sources to a uniform format. This process is called *normalization*. The events are then filtered, aggregated, and sent to the correlator service for analysis and to the storage service where they are retained. When KUMA recognizes a specific event or a sequence of events, it creates *correlation events*, which are also analyzed and retained. If an event or sequence of events indicates a potential security threat, KUMA creates an alert. This alert consists of a warning about the threat and all related data that should be investigated by a security officer. If the nature of the data received by KUMA or the generated correlation events and alerts indicate a possible attack or vulnerability, the symptoms of such an occurrence can be combined into an incident. Events can also be sent to the correlator for a retrospective scan.

You can view received events to investigate security threats or create correlation rules in the **Events** section. The events table displays the data received after the SQL query is executed.

To learn more about managing events, watch this video:

https://www.youtube.com/watch?v=WDLiCAaDX0M

For convenience of investigating alerts and processing incidents, make sure that time is synchronized on all devices involved in the event life cycle (event sources, KUMA servers, client hosts) with the help of Network Time Protocol (NTP) servers.

Event life cycle

Throughout their life cycle, events undergo conversions and may receive different names.

Event life cycle

The first steps are carried out in a collector:

1. Raw event. The original message from an event source received at a KUMA connector is called a *raw event*. This message is unprocessed, and KUMA cannot use it yet. To make it usable, it must be normalized to fit the KUMA data model.

2. Normalized event. A normalizer transforms the data of the raw event to make it fit the KUMA data model. After this transformation, the raw event becomes *normalized* and can be analyzed in KUMA. From this point on, KUMA handles only normalized events. Raw events are no longer used, but they can be kept as a part of normalized events inside the `Raw` field.

   The solution has the following normalizers:

   - JSON
   - CEF
   - Regexp
   - Syslog (as per RFC3164 and RFC5424)
   - CSV/TSV
   - Key-value
   - XML
   - Netflow v5, v9, IPFIX (v10), sFlow v5
   - SQL

   At this point, normalized events can already be used for analysis.

3. Event destination. After the collector has processed an event, it is ready to be sent to a KUMA correlator and/or storage.

The next steps of the event life cycle are completed in the correlator.

Event types

- Base event. An event that has been normalized.
- Aggregated event. When dealing with a large number of similar events, you can "merge" them into a single event to save processing time and resources. These act as base events and are processed in the same way, but In addition to all of the parameters of the parent events (the events that have been "merged"), an aggregated event has a counter that tells how many parent events it represents. Aggregated events also store the time when the first and last parent events were received.
- Correlation event. When a sequence of events is detected that satisfies the conditions of a correlation rule, the solution creates a *correlation event*. These events can be filtered, enriched, and aggregated. They can also be sent for storage or looped into the correlator pipeline.
- Audit events. Such events are created when certain security-related actions are performed in KUMA; such events are used to ensure system integrity. These events are automatically placed in a separate storage space and stored for at least 365 days.
- Monitoring events. Events that are used to monitor changes in the amount of data received by KUMA.

Filtering and searching events

By default, no data is displayed in the **Events** section of the web interface. To view events, you need to define an SQL query in the search field and click the **Run query** button. The SQL query can be entered manually or it can be generated using a query builder.

Data aggregation and grouping is supported in SQL queries.

You can search for events across multiple storages. For example, you can find events to determine where a user account is being blocked or which IP addresses were used to log in to which URLs.

Example of a query to search for events of a blocked user account

```
SELECT Timestamp, DestinationUserName, DeviceEventClassID, Message
FROM `events`
WHERE DestinationUserName = 'username'
   AND DeviceEventClassID = '4625'
LIMIT 250
```

To search for events in multiple storages, in the drop-down list in the upper-right part of the **Events** section, select check boxes next to the storages you want to search.

The list displays the following storages:

- Storages of the Main tenant.
- Available storages of tenants that satisfy one of the following conditions:
  - The tenant that owns the storage is enabled in the tenant filter and the user has permissions to read events in this tenant.
  - The user has access to the tenant of one of the storage partitions and has permission to read events in that tenant.

    For example, if you have access to the collector tenant, but do not have access to the storage tenant, by default, the inaccessible tenant's storage is not displayed in the list of available storages. If a destination in the storage of a tenant that is not available to you is added to the collector of an available tenant, after an event arrives in the partition of the tenant of the collector, the storage of the unavailable tenant appears in the list of storages in the **Events** section.

The drop-down list of storages in the upper-right part of the **Events** section displays the name of the first of the selected storages and the number of selected storages, if there are more than one. You can hover over the drop-down list to display all of the selected storages. If a space in a storage is deleted, the drop-down list of storages displays `deleted<ID of the deleted space>`. Events remain searchable until their TTL runs out.

The tenants selected in the tenant filter affect which storages are displayed in the drop-down list of storages. If you disable tenants whose storages are available to you in the tenant filter, these storages are no longer displayed in the drop-down list of storages. If these storages had been selected in the drop-down list of storages, their check boxes are cleared and events from these storages are not displayed. If only one storage is selected in the drop-down list of storages that is not from the Main tenant, and if in tenant selection you disabled the tenant that owns the selected storage, this storage is not displayed in the list of storages and KUMA automatically changes the selection to one of the storages of the Main tenant.

A simple query to all selected storages is allowed, as in the example above. If at least one of the selected storages is not available for the query, KUMA returns an error.

Limitations for searching events across multiple storages:

- When querying multiple storages, export to TSV, retrospective scan, and REST API requests are not available.
- The `SELECT` clause can contain only `*` and/or names of event fields. Aliases, functions, expressions are not allowed.
- The `ORDER BY` clause must also contain only event fields (no functions, constants, or expressions). If a field is not present in the list of fields for the `SELECT` clause, such a field is automatically added when sending to a specific cluster. You cannot set an `ORDER BY ClusterID`.
- `GROUP BY` is not available.

Complex queries with grouping and aggregation are allowed for a single selected storage.

You can add filter conditions to an already generated SQL query in the window for viewing statistics, the events table, and the event details area:

Changing a query from the Statistics window

*To change the filtering settings in the **Statistics** window:*

1. Open **Statistics** details area by using one of the following methods:

   - In the ••• drop-down list in the top right corner of the events table select **Statistics**.
   - In the events table click any value and in the opened context menu select **Statistics**.

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

2. Open the drop-down list of the relevant parameter and hover your mouse cursor over the necessary value.

3. Use the plus and minus signs to change the filter settings by doing one of the following:

   - If you want the events selection to include only events with the selected value, click the + icon.
   - If you want the events selection to exclude all events with the selected value, click the — icon.

   As a result, the filter settings and the events table will be updated, and the new search query will be displayed in the upper part of the screen.

Changing a query from the events table

To change the filtering settings in the events table:

1. In the **Events** section of the KUMA web interface, click any event parameter value in the events table.

2. In the opened menu, select one of the following options:

   - If you want the table to show only events with the selected value, select **Filter by this value**.
   - If you want to exclude all events with the selected value from the table, select **Exclude from filter**.

   As a result, the filter settings and the events table are updated, and the new search query is displayed in the upper part of the screen.

Changing a query from the Event details area

To change the filter settings in the event details area:

1. In the KUMA web interface, in the **Events** section, click the relevant event.

   The **Event details** area appears in the right part of the window.

2. Change the filtering settings by clicking the plus or minus icons:

   - If you want to apply the filter instantly and update the events table, click + or — next to the parameters that you need.
   - If you want to continue to change filtering parameters, hold down the `Ctrl` key and click + or —. This adds the condition to the body of the query, but does not automatically run the query.

When adding a condition to the query, an expression for the selected parameter is added to the `WHERE` clause. When adding conditions for multiple parameters, the expressions are joined with the `AND` operator. A field to be filtered by is added to the `SELECT` clause only if the `*` character is not used in the query.

Example of original query

```
SELECT Timestamp, Severity, Message
FROM `events`
ORDER BY Timestamp DESC
LIMIT 250
```

All events are selected without filters, the last 250 events are displayed in descending order by the `Timestamp` field.

When adding new conditions by **`Ctrl`**-clicking the + icon, the query looks like this:

```
SELECT Timestamp, Severity, Message, DeviceProduct, StartTime
FROM `events`
WHERE DeviceProduct = 'Windows'
   AND StartTime = 1755767943436
ORDER BY Timestamp DESC
LIMIT 250
```

Conditions are added to the `WHERE` clause with the `AND` operator. The `DeviceProduct` and `StartTime` fields were not included in the original `SELECT` clause, therefore they were added to the list of selected fields. The query is not executed automatically.

3. After adding all the necessary filtering conditions, run the query in one of the following ways:

   - Add the last condition without holding down the **`Ctrl`** key. The query is run automatically.
   - Close the event details area and run the query manually by clicking **Run query** button or pressing **`Ctrl+Enter`**.

   The filter settings and the events table are updated, and the modified search query is displayed in the upper part of the screen.

After modifying a query, all query parameters, including the added filter conditions, are transferred to the query builder and the search field.

When you switch to the query builder, the parameters of a query entered manually in the search field are not transferred to the builder, so you will need to create your query again. Also, the query created in the builder does not overwrite the query that was entered into the search string until you click the **Apply query** button in the builder window.

In the SQL query input field, you can enable the display of control characters.

You can also filter events by time period. Search results can be automatically updated.

The filter configuration can be saved. Existing filter configurations can be deleted.

Filter functions are available for users regardless of their roles.

When accessing certain event fields with IDs, KUMA returns the corresponding names.

For more details on SQL, refer to the ClickHouse documentation. For SQL operators and functions supported in KUMA, see also the KUMA operator usage and supported functions.

An event search generates an audit event for queries that are started manually.

An audit event is not generated for queries triggered by dashboards, reports, and data collection and analysis rules. REST API requests for receiving events also do not generate audit events. When using an `GROUP BY` option, opening a group generates an audit event because an additional query is executed at that time. When the **Run** option is selected, two audit events are generated in the background: Attempt to read events and Search query canceled.

If there is not enough RAM to complete the request, an error message is displayed.

Selecting Storage

Events that are displayed in the **Events** section of the KUMA web interface are retrieved from a storage (from the ClickHouse cluster). Depending on the demands of your company, you may have more than one Storage. However, you can only receive events from one Storage at a time, so you must specify which one you want to use.

To select the Storage you want to receive events from,

In the **Events** section of the KUMA web interface, open the drop-down list of storages in the upper right part of the section and select one or more spaces of one or more storages.

The list displays the following spaces:

- Spaces added when the storage service was created.
- The KUMA Default space.
- The KUMA Audit space, if the Main tenant is selected and if there is at least one audit event in this space.

KUMA displays only those spaces to which the user has access permissions.

Events from the selected storage are displayed in the table of events. Names of the selected storages are displayed in the drop-down list.

If you have access rights to the space that stores events of a tenant to which you do not have access permissions, such a space is displayed in the list, but is not searchable.

Generating an SQL query using a builder

In KUMA, you can use a query builder to generate an SQL query for filtering events.

To generate an SQL query using a builder:

1. In the **Events** section of the KUMA web interface, click the button.

   The filter constructor window opens.

2. Generate a search query by providing data in the following parameter blocks:

   SELECT—event fields that should be returned. The * value is selected by default, which means that all available event fields must be returned. To make viewing the search results easier, select the necessary fields in the drop-down list. In this case, the data only for the selected fields is displayed in the table. Note that Select * increases the duration of the request execution, but eliminates the need to manually indicate the fields in the request.

   When selecting an event field, you can use the field on the right of the drop-down list to specify an alias for the column of displayed data, and you can use the right-most drop-down list to select the operation to perform on the data: **count**, **max**, **min**, **avg**, **sum**.

   If you use aggregation functions in an SQL query, you can customize the display of columns in the event table. After executing the query without *, the columns will match the query.

   If the query uses grouping or aggregation functions, instead of one number that was received as a response to the `SELECT max(BytesOut) FROM `events` LIMIT 250` query, the radar shows a distribution of events from which this number is obtained.

   > When filtering by alert-related events in alert investigation mode, you cannot perform operations on the data of event fields or assign names to the columns of displayed data.

   - **FROM**—data source. Select the **events** value.

   - **WHERE**—conditions for filtering events.

     Conditions and groups of conditions can be added by using the **Add condition** and **Add group** buttons. The **AND** operator value is selected by default in the group of conditions, but you can change the operator by clicking it. Available values: **AND**, **OR**, **NOT**. The structure of conditions and condition groups can be changed by using the icon to drag and drop expressions.

     Adding filter conditions:

     a. In the drop-down list on the left, select the event field that you want to use for filtering.

     b. Select the necessary operator from the middle drop-down list. The available operators depend on the type of value of the selected event field.

     c. Enter the value of the condition. Depending on the selected type of field, you may have to manually enter the value, select it from the drop-down list, or select it on the calendar.

     You can delete filter conditions and filter condition groups by clicking .

   - **GROUP BY**—event fields or aliases to be used for grouping the returned data.

     If you use data grouping in an SQL query, custom fields specified in the query are displayed in the list of events. Table columns in a group cannot be customized. In group events, you can customize the display of columns.

     > When filtering by alert-related events in alert investigation mode, you cannot group the returned data.

   - **ORDER BY**—columns used as the basis for sorting the returned data. In the drop-down list on the right, you can select the necessary order: **DESC**—descending, **ASC**—ascending.

- **LIMIT**—number of strings displayed in the table.

  The default value is 250.

  If you are filtering events by user-defined period and the number of strings in the search results exceeds the defined value, you can click the **Show next** button to display additional strings in the table. This button is not displayed when filtering events by the standard period.

3. Click **Apply query**.

   The current SQL query will be overwritten. The generated SQL query is displayed in the search field.

   If you want to reset the builder settings, click the **Default query** button.

   If you want to close the builder without overwriting the existing query, click the button × in the upper right part of the query creation window.

4. Click the **Run query** button to display the data in the table.

   You can also run the query in the background. To do this, click the arrow icon next to the **Run query** button and click the **Run in background** button. In this case, the following happens:

   - The query is queued for execution in the background, and a task is created in the **Task Manager** section to run this query.
   - Background queries run in parallel at low priority.
   - A query containing more than 10,000 events cannot be queued for execution in the background.

   The table will display the search results based on the generated SQL query. You can view the result of running the query in the background in the **Task manager** section.

   If necessary, you can cancel the query. To do this, click the arrow icon next to the **Run query** button and select **Cancel query**. When a query is canceled, an audit event is automatically generated.

When switching to another section of the web interface, the query generated in the builder is not preserved. If you return to the **Events** section from another section, the builder will display the default query.

For more details on SQL, refer to the ClickHouse documentation. See also KUMA operator usage and supported functions.

Manually creating an SQL query

You can use the search field manually to create SQL queries of any complexity to filter events.

To manually generate an SQL query:

1. Go to the **Events** section of the KUMA web interface.

   An input form opens.

2. Enter your SQL query into the input field. You must use single quotes in your queries.

   When you enter a function name in the SQL query field, a list of available functions is displayed. For the selected function, a tooltip with a usage example is displayed to the right of it. For example, for the `concatWithSeparator` function, the following example is displayed: `concatWithSeparator('a', '1', '2', '3')`.

3. Click the **Run query** button.

   You can also run the query in the background. To do this, click the arrow icon next to the **Run query** button and select **Run in background**. In this case, the following happens:

   - The query is queued for execution in the background, and a task is created in the **Task Manager** section to run this query.
   - Background queries run in parallel at low priority.
   - A query containing more than 10,000 events cannot be queued for execution in the background.

   The table will display the search results based on the generated SQL query. You can view the result of running the query in the background in the **Task manager** section.

   If necessary, you can cancel the query. To do this, click the arrow icon next to the **Run query** button and select **Cancel query**. When a query is canceled, an audit event is automatically generated.

   If necessary, you can filter events in the table by period.

Supported functions and operators

Function	Description
`SELECT`	Event fields that you want to be returned. The following functions and operators are supported: • Aggregation functions: `count`, `avg`, `max`, `min`, `sum`. • Arithmetic operators: `+`, `-`, `*`, `/`, `<`, `>`, `=`, `!=`, `>=`, `<=`. You can combine functions and operators in an SQL query. If you use aggregation functions in an SQL query, you can customize the display of columns in the event table. After executing the query without *, the columns will match the query. If the query uses grouping or aggregation functions, instead of one number that was received as a response to the `SELECT max(BytesOut) FROM `events` LIMIT 250` query, the radar shows a distribution of events from which this number is obtained.
`FROM`	Data source. When creating an SQL query, you need to specify the events value as the data source.
`WHERE`	Conditions for filtering events: • `AND`, `OR`, `NOT`, `=`, `!=`, `>`, `>=`, `<`, `<=` • `IN` • `BETWEEN` • `LIKE` • `ILIKE` • `inSubnet` • `match` (the re2 syntax of regular expressions is used in SQL queries) You must additionally escape special characters with the backslash `\`.
`GROUP BY`	Event fields or aliases to be used for grouping the returned data. If you use data grouping in an SQL query, custom fields specified in the query are displayed in the list of events. Table columns in a group cannot be customized. In group events, you can customize the display of columns.

Function	Description
`ORDER BY`	Columns by which you want to sort the returned data. Possible values: • `DESC` to sort in descending order • `ASC` to sort in ascending order
`OFFSET`	The number of rows to skip before displaying the results of the SQL query.
`LIMIT`	The number of rows that can be displayed in the table. The default value is `250`. If you are filtering events by user-defined period and the number of rows in the search results exceeds the defined value, you can click the **Show next** button to display additional rows in the table. This button is not displayed when filtering events by the standard period.

Examples of SQL queries

- `SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250`
  In the events table, all events with the **Base** and **Audit** type are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.
- `SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250`
  All events of the events table for which the **BytesIn** field contains a value of received traffic in the range from 1,000 to 2,000 bytes are sorted by the **Timestamp** column in ascending order. The number of strings that can be displayed in the table is 250.
- `SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250`
  In the events table, all events whose **Message** field contains data corresponding to the defined `%ssh:%` template in lowercase are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.
- `SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250`
  In the events table, all events for the hosts that are in the 00.0.0.0/00 subnet are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.
- `SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250`
  In the events table, all events whose **Message** field contains text corresponding to the `ssh.*` template are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.
- `SELECT max(BytesOut) / 1024 FROM `events``
  Maximum amount of outbound traffic (KB) for the selected time period.
- `SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250`
  Number of events and port number. Events are grouped by port number and sorted by the **Port** column in ascending order. The number of strings that can be displayed in the table is 250.
  The **ID** column in the events table is named Count, and the **SourcePort** column is named Port.

If you want to use a special character in a query, you need to escape this character by placing a backslash (\) character in front of it.

Example:

```
SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250
```

In the events table, all events whose **Message** field contains text corresponding to the `ssh: 'connection'` template are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.

When creating a normalizer for events, you can choose whether to retain the field values of the raw event. The data is stored in the **Extra** event field. This field is searched for events by using the LIKE operator.

Example:

```
SELECT * FROM `events` WHERE DeviceAddress = '00.00.00.000' AND Extra LIKE '%"app":"example"%' ORDER BY Timestamp DESC LIMIT 250
```

In the events table, all events for hosts with the IP address 00.00.00.000 where the example process is running are sorted by the **Timestamp** column in descending order. The number of strings that can be displayed in the table is 250.

If you created an SQL query manually in the search field and then switched to the builder, the SQL query parameters are not transferred to the builder. In this case, you will need to re-create the SQL query in the builder. The SQL query created in the builder does not overwrite the SQL query that was entered into the search string until you click the **Apply query** button in the builder window. If you created an SQL query in the query builder and then switched to the search field, the query parameters are transferred automatically.

Aliases must not contain spaces.

For more details on SQL, refer to the ClickHouse documentation. See also the supported ClickHouse functions.

Building a process chain using an SQL query

When investigating incidents, it may be necessary to analyze the sequence in which processes were started on the endpoint and determine the relationship between parent and child processes.

Windows process creation events with ID 4688 contain information about the started process and its parent process. You can use an SQL query to correlate process creation events and get a three-tier chain: GrandParent → Parent → Current.

The query correlates process creation events by process IDs and generates a textual representation of the chain in the `ProcessTree` field.

As a result, you can get the following information:

- Endpoint name
- User account and user name
- IDs and names of processes at the grandparent, parent, and current tiers
- The process spawning sequence in the `ProcessTree` field.

To build a chain of processes:

1. In the web interface, go to the **Events** section.
2. Using the query builder or manually, enter the following query in the text box:

```
SELECT
    b.DeviceHostName AS HostName,
    b.SourceAccountID AS AccountID,
    b.SourceUserName AS UserName,
    a.DeviceCustomString3 AS GrandParentProcessID,
    a.SourceProcessName AS GrandParentProcessName,
    a.DeviceCustomString5 AS ParentProcessID,
    a.DestinationProcessName AS ParentProcessName,
    b.DeviceCustomString5 AS ProcessID,
    b.DestinationProcessName AS ProcessName,
    CONCAT(
        a.SourceProcessName,
        ' -> ',
        a.DestinationProcessName,
        ' -> ',
        b.DestinationProcessName
    ) AS ProcessTree
FROM `events` AS a
INNER JOIN (
    SELECT *
    FROM `events`
    WHERE DeviceEventClassID = '4688'
) AS b
ON a.DeviceCustomString5 = b.DeviceCustomString3
WHERE a.DeviceEventClassID = '4688';
```

3. In the upper part of the window, open the time period drop-down list and specify a time range that you want to search for events.

4. Click the **Run query** button.

   After running the query, a table with the results is displayed in the workspace.

   Example of a query result table

Description of query result fields

Field	Description
`HostName`	Name of the endpoint on which the event occurred.
`AccountID`	ID of the user account that started the process.
`UserName`	Name of the user that started the process.
`GrandParentProcessID`	Process identifier of the topmost process in the chain.
`GrandParentProcessName`	Name of the topmost process in the chain.
`ParentProcessID`	Parent process identifier.
`ParentProcessName`	Name of the parent process.
`ProcessID`	ID of the current child process.
`ProcessName`	Name of the current child process.
`ProcessTree`	Textual representation of the process chain in the format: GrandParent → Parent → Current. The `ProcessTree` field can have a value like `explorer.exe` → `cmd.exe` → `powershell.exe`. In this case, `explorer.exe` is the topmost process, `cmd.exe` is its child process, and `powershell.exe` is the child process of `cmd.exe`.

5. If you want to reuse the SQL query, save it:

   a. Save the query by clicking the floppy disk icon.

   b. This opens a window; in that window, enter a name, for example, `Process chain (4688)`.

   c. Select the folder in which you want to save this query.

   d. Click the **Save** button.

      You can find the saved query by clicking the bookmark icon.

After running the query, make sure that:

- The results display process creation events with `DeviceEventClassID = '4688'`.
- The value of the `ParentProcessID` field corresponds to the process identifier of the parent process.
- The value of the `ProcessID` field corresponds to the process identifier of the current process.
- The `ProcessTree` field contains a sequence of three related processes.
- The host and user details match the raw events.

As a result of running the query, you get a sequence of processes that you can use to analyze the relationships between processes on the endpoint.

Saving query history

In the KUMA web interface, the **Events** section keeps a personal history of SQL search queries. You can refer to the history of queries and quickly find a query you have used in the past.

The queries are saved in the browser. Changing your browser resets the query history. The history stores the last 32 of your queries. Queries are displayed with formatting. The date and time when the query was executed is displayed.

Only queries with correct syntax are saved in the query history.

To find a search query in history:

1. In the **Events** section, place the cursor in the query bar.
2. Click the (**SQL history**) button in the toolbar of the query window or press **Ctrl+]** or **Ctrl+[**.

   This opens the query history window. The last query you ran is displayed at the top of the list of queries.
3. Select a search query. To navigate the list of saved queries, press **`Ctrl`**+**`]`** or **`Ctrl`**+**`[`**.

   The selected query is pasted to the search bar.
4. If necessary, run the search query. To do so, press **`Ctrll`**+**`Enter`**.

When you run a query, the query history window is closed.

You can also close the query history window by pressing the **`Esc`** key; this moves the cursor to the query editing window.

You can copy the query to the clipboard by pressing **`Ctrl`**+**`C`**. This copies the part of the query that is highlighted with the mouse, or the entire query string, limited by the box, if there was no selection.

You can save the query by pressing **`Ctrl`**+**`S`**, or by clicking the button (**Save query**) in the row. This closes the history window and opens the sidebar for saving the query with populated fields.

You can paste a query into the query window without running it by clicking the (**Insert query**) button, or by pressing **`Enter`**.

Managing saved search queries

In KUMA, in the **Events** section, you can organize saved SQL queries in a tree of folders for structured storage and quick search of SQL queries. You can edit previously saved queries, rename them, arrange queries in groups (folders) of accessible tenants, and search for previously saved queries in the search bar.

Saved queries follow the tenant access model and are visible to all users that have access to the corresponding tenants.

Saved queries are placed in the **Saved queries pane.** You can open or close the **Saved queries** pane using the (bookmark) button on the toolbar of the query window.

The **Saved queries** navigation pane on the left contains the following:

- The query search window where you can search by folder name and query name.
- Tree of folders and queries, the **Favorites** folder.
- The query filter that displays the queries you have created (on the **My** tab) and all queries (on the **All** tab)

Displaying a query in the query window

To display a query in the query window:

1. In the **Events** section, click the (bookmark) button.
   This opens the **Saved queries** navigation pane.
2. In the tree of folders in the **Saved queries** pane, click to select the relevant query.

The text of the selected query is displayed in the query window.

Saving a query to a folder or a tenant

In the **Events** section, after entering a query in the query window and clicking the **Save current query** button (floppy disk icon), you can save the SQL query to one of the folders or tenants that you can select.

To save a query to a folder:

1. In the **New search** window, in the **Filter name** field, enter a name for the filter.
   Consider the following when naming the filter:
   - The name can contain Unicode characters.
   - The minimum length of a name is 1 character, and the maximum length is 128 characters.
   - Names must be unique within a tenant.
   - Tab characters, new line characters, and paragraph characters are replaced with space characters.

   When saving the name:
   - Leading and trailing spaces are removed.
   - Multiple spaces between characters are replaced with a single space character.
2. In the **Query** field, enter the text of the SQL query.

3. Select a tenant, a folder from the list of folders created in the tenant that is available to you, or create a new folder by clicking the **Add folder** button.

   You can also add a folder in the **Saved queries** window: click the + button next to the tenant to open the **New folder** window and add the folder in that window.

4. Click the **Save** button.

The query is saved in the selected folder or tenant.

Viewing the text of a query

To view the text of a query:

1. In the **Events** section, click the (bookmark) button.

   This opens the **Saved queries** navigation pane.

2. In the tree of folders in the **Saved queries** pane, click the button next to the relevant query.

This opens a window with the text of the query.

Setting the default query

You can set your default query that the **Events** section displays when opened.

To set the default query:

1. In the **Events** section, click the (bookmark) button.

   This opens the **Saved queries** navigation pane.

2. In the tree of folders on the **Saved queries** pane, select the relevant query.

3. Click the button and in the displayed menu, select **Use by default**.

The selected query becomes the default query.

Adding folders and queries to favorites

To add a folder or individual query to favorites:

1. In the **Events** section, click the (bookmark) button.

   This opens the **Saved queries** navigation pane.

2. In the tree of folders in the **Saved queries** pane, select the relevant folder or query.
3. Click the ⋮ button and in the displayed menu, select **To favorites**.

   The selected folder or resource is added to the **Favorites** folder.

Editing a query

To edit a query:

1. In the **Events** section, click the (bookmark) button.
   This opens the **Saved queries** navigation pane.
2. In the tree of folders on the **Saved queries** pane, select the relevant query.
3. Click the ⋮ button and in the displayed menu, select **Edit**.
   This opens the window for editing the saved query.
4. In the window, edit the query name or text, or the folder in which you want to save the query.
5. Click the **Save** button.

   The query is updated and saved in the selected folder.

Deleting a query

To delete a query from a folder (if you have sufficient rights):

1. In the **Events** section, click the bookmark ( ) icon.
   This opens the **Saved queries** navigation pane.
2. In the tree of folders on the **Saved queries** pane, select the relevant query.
3. Click the three-dot icon (⋮) and in the menu that appears, select **Delete**.
4. Confirm deletion in the displayed window.

   The query is deleted.

Searching for related events

You can search for events processed by the Correlator or the Collector services.

To search for events related to the Correlator or the Collector service:

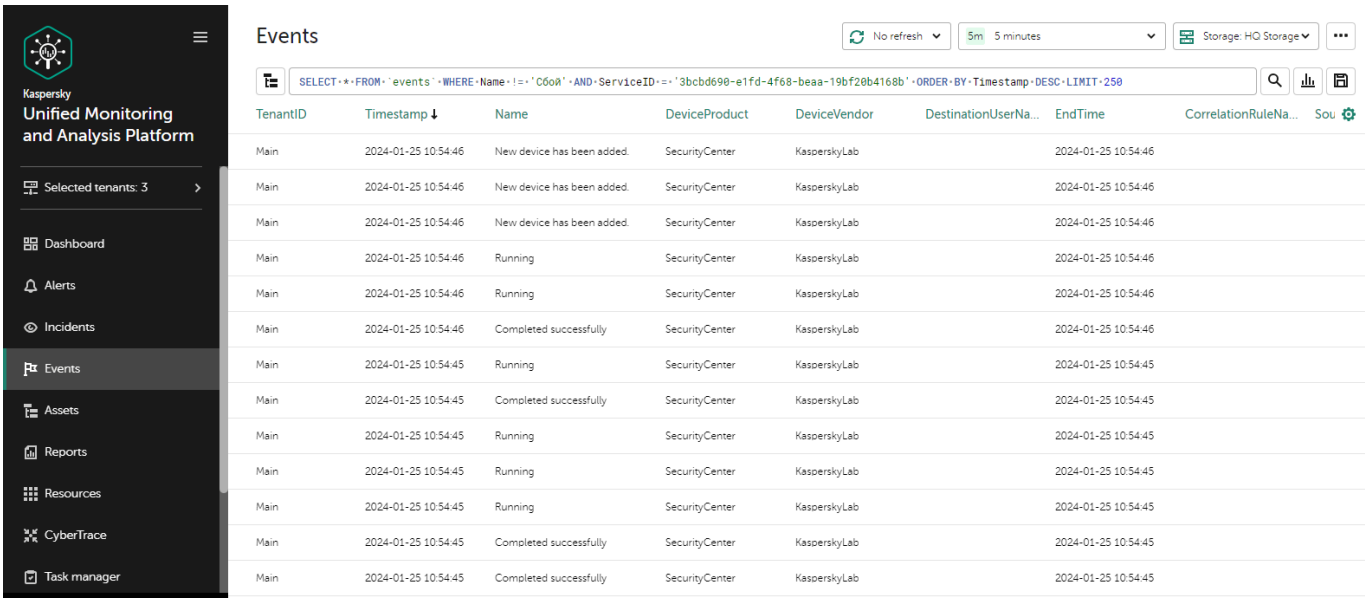
1. Log in to the KUMA web interface and open **Resources** → **Active services**.

2. Select the check box next to the required correlator or collector and click **Go to Events**.

   This opens a new browser tab with the KUMA **Events** section open.

3. To find events, click the icon.

   A table with events selected by the `ServiceID = <ID of the selected service>` search expression is displayed.



Event search results

When searching for events, you may encounter the following shard unavailability error:

```
Code: 279. DB::NetException: All connection tries failed. Log: \\n\\nTimeout exceeded
while connecting to socket (host.example.com:port, connection timeout 1000 ms)\\nTimeout
exceeded while connecting to socket (host.example.com:port, connection timeout 1000
ms)\\nTimeout exceeded while connecting to socket (host.example.com:port, connection
timeout 1000 ms)\\n\\n: While executing Remote. (ALL_CONNECTION_TRIES_FAILED) (version
23.8.8.207)\\n\"}",
```

In this case, you need to override the ClickHouse configuration in storage settings.

To override the ClickHouse configuration:

1. In the KUMA web interface, select the **Resources** section.

2. In the **Services configuration** → **Storages** section, click the storage resource that you want to edit.

   This opens the **Edit storage** window.

3. In the **ClickHouse configuration override** field, specify the following settings:

   - To skip unavailable shards when searching, insert the following lines:

```
<profiles>
        <default>
                <skip_unavailable_shards>1</skip_unavailable_shards>
        </default>
```

```
</profiles>
```

- To set memory usage limits, specify `max_server_memory_usage` or `max_memory_usage_for_all_queries` parameters as recommended.

4. To apply the ClickHouse configuration, click **Save**.

5. Restart the storage services that depend on this resource.

   This resolves the shard unavailability error, and you can proceed to search for events processed by a particular correlator or collector.

Searching for events using account and asset information

When analyzing events, you can use not just the event fields, but also information about associated accounts and assets.

The `lookup_accounts`, `lookup_assets`, and `enrich_accounts` functions filtering events by attributes of accounts and assets and get additional information about these objects. This approach allows accounting for the context of the event: the department and job of the user and the manager, the department to which the asset belongs, and other attributes.

The following example searches for failed login attempts. Events are selected based on the values of the attributes of the source asset and the target account; the value of the `Manager` attribute of the target account is added to the result.

> The `Accounting`, `IT`, and `sysadmin` values in the query are examples. Replace these with values that correspond to the attributes of accounts and assets in your infrastructure.

Before using the query, make sure that event enrichment with account and asset data is configured in Kaspersky SIEM and that the attributes used in the request are actually filled in.

The scenario proceeds in stages:

1 Creating an SQL query

To create an SQL query:

1. In the KUMA web interface, go to the **Events** section.

2. Using the query builder or manually, enter the following query in the text box:

```
SELECT
    enrich_accounts(DestinationAccountID, manager) AS manager
FROM events
WHERE DeviceEventClassID = 4625
    AND lookup_assets(SourceAssetID, Department, '=', 'Accounting')
    AND lookup_accounts(DestinationAccountID, Division, '=', 'IT')
    AND lookup_accounts(DestinationAccountID, Title, '=', 'sysadmin')
```

3. If necessary, replace the `Accounting`, `IT`, and `sysadmin` values with the values used in the properties of assets and accounts in your infrastructure.

4. In the upper part of the window, open the time period drop-down list and specify a time range that you want to search for events.

5. Click the **Run query** button.

2 Analyzing query results

The query returns a list of values for the `manager` field.

Make sure that the query does the following:

- Selects events with `DeviceEventClassID = 4625`.
- Uses the `lookup_assets` function to filter events based on the `Department` attribute of the source asset.
- Uses the `lookup_accounts` function to filter events by the `Division` and `Title` attributes of the target account.
- Uses the `enrich_accounts` function to get the value of the `Manager` attribute of the target account.

You can specify search conditions not only by event fields, but also by the attributes of the associated accounts and assets.

3 Configuring search conditions (optional step)

Modify the query conditions if necessary.

Settings of query conditions

Setting	Description
`DeviceEventClassID = 4625`	Select events with the specified event class ID.
`lookup_assets(SourceAssetID, Department, '=', 'Accounting')`	Select events by the `Department` attribute of the source asset.
`lookup_accounts(DestinationAccountID, Division, '=', 'IT')`	Select events by the `Division` attribute of the target account.
`lookup_accounts(DestinationAccountID, Title, '=', 'sysadmin')`	Select events by the `Title` attribute of the target account.
`enrich_accounts(DestinationAccountID, manager)`	Get the value of the `Manager` attribute of the target account.

You can change the `lookup_assets` and `lookup_accounts` conditions in accordance with the goals of your analysis. You can use different attributes of accounts and assets, or change the values that are used for filtering.

4 Verifying the result

After running the query, make sure that:

- Only events that match the specified conditions are present in the results.
- Events are filtered by attributes of associated assets and accounts.
- The `manager` field contains the value of the `Manager` attribute of the corresponding account.

If the test event satisfies all conditions of the query, the `Manager` value of the target account should be present in the query result.

Filtering events by period

In KUMA, you can specify the time period to display events from.

To filter events by period:

1. In the **Events** section of the KUMA web interface in the upper part of the window, open the time period drop-down list in the top right part of the section.
2. Select a period in one of the following ways:
   - If you want to specify an **exact date**, select start and end dates of the period in the calendar and click **Apply**.

     You can select a date up to and including the current date. The date and time format depends on your browser settings. If the **Range from** or **Range to** field has a value and you have not edited the time value manually, when you select a date in the calendar, the **Range from** field is automatically populated with `00:00:00,000`, and the **Date to** field is populated with `23:59:59,999`. If you have manually deleted the value in the **Range from** or **Range to** field, when you select a date in the calendar, the field is automatically populated with the current time. Once you select a value in one of the fields, the focus switches to the other field. If your **Range to** is earlier than your **Range from**, this earlier value is automatically inserted into the **Range from** field.
   - If you want to specify a **relative period**, select one of the periods available in the **Relative period** list.

     The period is calculated relative to the current time.
   - If you want to specify a **custom period**, set or edit the value of the **Range from** and **Range to** fields manually.

     You can enter an exact date and time in the `DD.MM.YYYY HH:mm:ss.SSS` format for the Russian localization and `YYYY-MM-DD HH:mm:ss.SSS` for the English localization or a period relative to the current time as a formula. You can also combine these methods. If you do not specify milliseconds when entering the exact date, `000` is substituted automatically. If you have edited the time in the **Range from** or **Range to** fields, picking a date in the calendar does not change the time component.

     In the relative period formulas, you can use the `now` parameter for the current date and time and the interval parameterization language: `+` (only in the **Range to** field), `-`, `/` (rounding to the nearest), as well as time units: `y` (year), `M` (month), `w` (week), `d` (day), `h` (hour), `m` (minute), `s` (second). For example, you can specify the period `now-5d` to get data for the last five days, or `now/w` to get data from the beginning of the first day of the current week (00:00:00:000 UTC) to the current time (`now`).

> The **Range from** field is required, and its value cannot exceed the value of the **Range to** field, and also cannot be earlier than 1970-01-01 (if specifying an exact date or a relative period). The **Range to** cannot be earlier than the **Range from**. If you do not specify a value in the **Range to** from field, `now` is specified automatically.

The default setting is **5 minutes** (**now-5m**). The bounds of the period are inclusive: for example, for the **Today** time range, events are displayed from the beginning (00:00:00:000 UTC) of the current day to the current time (**now**) inclusive, and for the **Yesterday** period, events are displayed from the beginning (00:00:00:000 UTC) of the previous day to 00:00:00:000 UTC of the current day.

KUMA stores time values in UTC, but in the user interface time is converted to the time zone of your browser. This is relevant to the relative periods: **Today**, **Yesterday**, **This week**, and **This month**. For example, if the time zone in your browser is UTC+3, and you select the **Today** period, events are displayed for the period from 03:00:00.000 until now, not from 00:00:00.000 until now.

If, when selecting a relative period, such as **Today**, **Yesterday**, **This week**, or **This month**, you want to take your time zone into account when displaying events, you need to manually add a time offset in the **Range from** and **Range to** fields (if a value other than **now** is specified) by adding or subtracting the correct number of hours. For example, if your browser's time zone is UTC+3 and you want to display data for **Yesterday**, you need to change **Range from** to **now-1d/d-3h** and **Date to** to **now/d-3h**. If you want to display data for the **Today** period, you only need to change the value in the **Range from** field to **now/d-3h**.

> If you need results up to 23:59:59:999 of yesterday, you can use an SQL query with a filter by Timestamp or specify an exact date and time.

3. If you want to capture the last relative period for which a query was executed as an exact date and time, click the button.

   The relative period is then converted to an exact date and time. Hovering over this button displays the date and time that will be captured. Relative periods (**Today**, **Yesterday**, **This week**, **This month**) are converted to an exact UTC date and time, other periods are converted to a date and time that takes into account the time zone of the browser.

   > If you have executed an SQL query with event grouping, when switching between groups in the query results, the relative time range is automatically converted to an exact date and time.

4. Click **Run query** to run the query.

   Only events registered during the specified time period are displayed. The period will be displayed in the upper part of the window.

You can also configure the display of events by using the events histogram that is displayed when you click the button in the upper part of the **Events** section. Events are displayed if you click the relevant data column or select the relevant time period and click the **Show events** button.

Displaying the list of events with a relative and absolute calendar period

The display of the list of events in the table in the **Events** section depends on the selected event filtering period: relative or absolute.

When a relative period is selected, the display is as follows:

- If a certain value is specified for the `LIMIT` variable in the SQL query, the number of displayed events corresponds to this value.

  Example SQL query: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 10`.

- If the `LIMIT` value is not specified in the SQL query, 250 events are displayed by default.

  Example SQL query: `SELECT * FROM `events` ORDER BY Timestamp DESC`.

> If a relative period is selected, all events are displayed on the same page.

If an absolute period is selected, the display is as follows:

- If the value of the `LIMIT` variable in the SQL query is less than or equal to 49, and more than 49 events are found, to view additional rows in the table, you need to click the **Show more** button.

  Example SQL query: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 48`.

- If the value of the `LIMIT` variable in the SQL query is greater than 49, and more than 49 events are found, additional events are loaded into the list automatically.

  Example SQL query: `SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 50`.

Grouping events

After getting a list of events, you often need to split the events into groups to localize an information security event. KUMA can group events in a list by one or more fields.

To group events, you no longer need to manually edit the text of the query; instead, you can click a column heading in the **Events** section and select **Add "Group by" in query** in the context menu. You can select a sequence of multiple fields to group by, and the fields will be automatically added to the query string. Having selected your fields, click **Run query**. As a result, events are grouped by the specified fields. Found groups are displayed in the **Groups** section. They can be displayed as a table and as cards. You can toggle between the display modes.

You can exclude a group from the query:

- In **Cards** mode, click the (`—`) button.

- In **Tables** mode, right-click the group and in the context menu, select **Exclude group from filter**.

As a result, the query is automatically modified and the group is excluded from the query.

If you want to go back to the original query, click **Return to initial select query**.

You can navigate through the groups and view the contents of each group.

You can do a global search in all groups or a local search in events within a selected group.

You can use more complex grouping by adding one or more fields.

You can remove a group from the grouping and in this way, go back one step.

If the grouping query returns many events, only the first 1000 events are displayed. If the query contains SELECT Count(ID), you can click the link with the total number of events in the query result to view all events. If the request does not contain Count(ID), the number of events in the group is not indicated, but you still can click the link and view the total number of events in the group.

Statistics, retrospective scan by group, and export to TSV are available.

If you want the grouping result to be independent of time (because events arrive continuously), you can set a fixed relative interval and apply it as an absolute interval so that the events of interest do not drop out of the selection. To fix a relative interval, in the **Events** section, in the time interval drop-down list, select **Apply current range**. You can now manage groups within this query.

If you want to arrange the selected events by months, days, minutes, and seconds, you can group events by the Timestamp field. To group events, select a grouping option in the context menu of the Timestamp field in the event table.

If you want to normalize the value of the Timestamp field and display the time values from different sources in the same UTC time scale, select **Convert to UTC timezone** in the context menu of the Timestamp field in the events table.

Displaying names instead of IDs

When accessing certain event fields with IDs, KUMA returns the corresponding names rather than IDs. This helps make the information more readable. For example, if you access the `TenantID` event field (which stores the tenant ID), you get the value of the `TenantName` event field (which stores the tenant name).

When exporting events, values of both fields are written to the file, the ID as well as the name.

The table below lists the fields that are substituted when accessed:

Requested field	Returned field
`TenantID`	`TenantName`
`ServiceID`	`ServiceName`
`DeviceAssetID`	`DeviceAssetName`
`SourceAssetID`	`SourceAssetName`
`DestinationAssetID`	`DestinationAssetName`
`SourceAccountID`	`SourceAccountName`
`DestinationAccountID`	`DestinationAccountName`

Substitution does not occur if an alias is assigned to the field in the SQL query, for example:

- `SELECT TenantID FROM `events` LIMIT 250` — in the search result, the name of the tenant is displayed in the `TenantID` field.
- `SELECT TenantID AS Tenant_name FROM `events` LIMIT 250` — in the search result, the tenant ID is displayed in the `Tenant_name` field.

Presets

You can use presets to simplify work with queries if you regularly view data for a specific set of event fields. In the line with the SQL query, you can type `Select *` and select a saved preset; in that case, the output is limited only to the fields specified in the preset. This method slows down performance but eliminates the need to write a query manually every time.
Presets are saved on the KUMA Core server and are available to all KUMA users of the specified tenant.

To create a preset:

1. In the **Events** section, click the icon.
2. In the window that opens, on the **Event field columns** tab, select the required fields.

   To simplify your search, you can start typing the field name in the **Search** area.
3. To save the selected fields, click **Save current preset**.

   The **New preset** window opens.
4. In that window, specify the **Name** of the preset, and in the drop-down list, select the **Tenant**.
5. Click **Save**.

   The preset is created and saved.

To apply a preset:

1. In the query entry field, enter **Select ***.
2. In the **Events** section of the KUMA web interface, click the icon.
3. In the opened window, use the **Presets** tab to select the relevant preset and click the button.

   The fields from the selected preset are added to the SQL query field, and the columns are added to the table. No changes are made in Builder.
4. Click **Run query** to run the query.

   After the query execution completes, the columns are filled in.

Limiting the complexity of queries in alert investigation mode

When investigating an alert, the complexity of SQL queries for event filtering is limited if **Related to alert** is selected in the drop-down list of event sources. If this is the case, only the functions and operators listed below are available for event filtering.

> If **All events** is selected from the drop-down list of event sources, these limitations do not apply.

- `SELECT`
  - The `*` character is used as a wildcard to represent any number of characters.

- `WHERE`
  - `AND, OR, NOT, =, !=, >, >=, <, <=`
  - `IN`
  - `BETWEEN`
  - `LIKE`
  - `inSubnet`

  Examples:

  - `WHERE Type IN ('Base', 'Correlated')`
  - `WHERE BytesIn BETWEEN 1000 AND 2000`
  - `WHERE Message LIKE '%ssh:%'`
  - `WHERE inSubnet(DeviceAddress, '10.0.0.1/24')`
- `ORDER BY`

  Sorting can be done by column.
- `OFFSET`

  Skip the indicated number of lines before printing the query results output.
- `LIMIT`

  The default value is 250.

  If you are filtering events by user-defined period and the number of strings in the search results exceeds the defined value, you can click the **Show next** button to display additional strings in the table. This button is not displayed when filtering events by the standard period.

When filtering by alert-related events in alert investigation mode, you cannot perform operations on the data of event fields or assign names to the columns of displayed data.

Saving and selecting events filter configuration

In KUMA, you can save a filter configuration and use it in the future. Other users can also use the saved filters if they have the appropriate access rights. When saving a filter, you are saving the configured settings of all the active filters at the same time, including the time-based filter, query builder, and the events table settings. Search queries are saved on the KUMA Core server and are available to all KUMA users of the selected tenant.

To save the current settings of the filter, query, and period:

1. In the **Events** section of the KUMA web interface, click the icon next to the filter expression.

   This opens the **New filter** window.
2. In the window that opens, enter the name of the filter configuration in the **Name** field. The name can contain up to 128 Unicode characters.

3. Under **Select folder**, select the tenant to which you want the created filter to belong and the folder inside the tenant, if necessary.

   To simplify your search, you can start typing the name in the **Search** area.

4. If necessary, click **Add folder** to create a new folder inside the selected tenant.

5. Click **Save**.

   The filter configuration is now saved.

To select a previously saved filter configuration:

In the **Events** section of the KUMA web interface, click the ☆ icon next to the filter expression and select the relevant filter.

The selected configuration is active, which means that the search field is displaying the search query, and the upper part of the window is showing the configured settings for the period and frequency of updating the search results. Click the **Run query** button to submit the search query.

To add the filter configuration to favorites, you can hover over the name of the filter configuration, click the ⋮ icon next to the name of the configuration and click the **To favorites** button.

Deleting event filter configurations

To delete a previously saved filter configuration:

1. In the **Events** section of the KUMA web interface, click the ☆ icon next to the filter search query.

   This opens the **Saved queries** window.

2. Hover over the configuration that you want to delete and click the ⋮ icon next to its name.

3. This opens a menu; in the menu, click the 🗑 icon.

   The filter configuration is now deleted for all KUMA users.

Supported ClickHouse functions

The following ClickHouse functions are supported in KUMA:

- Arithmetic functions.
- Arrays.
- Comparison functions.
- Logical functions.
- Type conversion functions.
- Date and time functions.

- String functions.
- String search functions.
- Conditional functions: only the regular 'if' operator; the ternary operator is not supported.
- Mathematical functions.
- Rounding functions.
- Functions for splitting and merging strings and arrays.
- Bit functions.
- Functions for working with UUIDs.
- Functions for working with URLs.
- Functions for working with IP addresses.
- Functions for working with Nullable arguments.
- Functions for working with geographic coordinates.

Functions from other sections are not supported.

For more details on SQL, refer to the ClickHouse documentation.

Viewing event detail areas

To view information about an event:

1. In the solution web interface window, select the **Events** section.
2. Search for events by using the query builder or by entering a query in the search field.
   The event table is displayed.
3. Select the event whose information you want to view.

   The event details window opens.

The **Event details** area appears in the right part of the web interface window and contains a list of the event's parameters with values. In this area you can:

- Include the selected field in the search or exclude it from the search by clicking + or – next to the setting value.
- Click a file hash in the **FileHash** field open a list in which you can select one of the following actions:
  - Show info from **Threat Lookup**.
    This is available when integrated with **Kaspersky Threat Intelligence Portal**.
  - Add to **Internal TI of CyberTrace**.
    This is available when integrated with **Kaspersky CyberTrace**.

- Open a window containing information about the asset if it is mentioned in the event fields and registered in the solution.

- Click the link containing the collector name in the **Service** field to view the settings of the service that registered the event.

  You can also link an event to an alert if the solution is in the alert investigation mode and open the **Correlation event details** window if the selected event is a correlation event.

- You can view all non-empty event fields by clicking **Show all event fields**. The following conditions must be satisfied for the rule to trigger:

  - The query is executed for a set of fields and is not a `SELECT *`.

  - Not all non-empty fields are displayed. If all non-empty fields are displayed in the event card, the **View all event fields** button is not displayed.

  - The event card is opened in KUMA in the **Events** section.

  This does not change the original query or rebuild the table of events.

  Displaying an event with populated Message, SourceAddress, and DeviceCustomString1 fields

  Preliminary condition: an event was sent with multiple non-empty fields, such as `Message`, `SourceAddress`, `DeviceCustomString1`.

  A query was executed for a set of fields:

  ```
  SELECT Type, Message
  FROM `events`
  ORDER BY Timestamp
  DESC LIMIT 250
  ```

  Clicking an event opens the **Event Information** window with the following information:

  - The `Type` and `Message` fields from the query.

  - The default `TenantID` and `Timestamp` fields not specified in the query.

  Non-empty `SourceAddress` and `DeviceCustomString1` fields of the event that are missing from the query but are present in the sent event are not displayed.

  To view all non-empty fields,

  click **View all event fields**.

  This displays all non-empty fields of the event: `Type`, `Message`, `TenantID`, `Timestamp`, `SourceAddress`, `DeviceCustomString1`.

- Enable or disable compact display for `*Label` fields by clicking on the gear icon ⚙ and enabling or disabling the toggle switch. By default, the toggle switch is set to **Full view**. When you set it to the **Compact view** position for the `DeviceCustom*` and `Flex*` fields, the value of the corresponding `*Label` field is displayed as a field alias, while the original field name is displayed under its value. If the `*Label` field has no value, the original field name is displayed. The selected display mode persists after refreshing the page and exiting the **Events** section.

- Change the display of the event by clicking the **Format** button. By default, the event is displayed as a one-line string in XML or JSON format. When you click this button, the event is displayed in multi-line format with indentation. Clicking the button again reverts the display to the one-line format. Formatting is applied to all events in the table in the **Events** section.

In the **Event details** area, the name of the described object is shown instead of its ID in the values of the following settings. At the same time, if you change the filtering of events by this setting (for example, by clicking — to exclude events with a certain setting-value combination from search results), the object's ID, and not its name, is added to the SQL query:

- `TenantID`
- `ServiceID`
- `DeviceAssetID`
- `SourceAssetID`
- `DestinationAssetID`
- `SourceAccountID`
- `DestinationAccountID`

Exporting events

In KUMA, you can export information about events to a TSV file. The selection of events that will be exported to a TSV file depends on filter settings. The information is exported from the columns that are currently displayed in the events table. The columns in the exported file are populated with the available data even if they did not display in the events table in the KUMA web interface due to the special features of the SQL query.

To export information about events:

1. In the **Events** section of the KUMA web interface, click the **TSV** button in the upper part of the table of events.

   The new export TSV file task is created in the **Task manager** section.

2. Find the task you created in the **Task manager** section.

   When the file is ready to be downloaded, the **Status** column of the task displays the **Completed** status and the icon.

3. Click the task type name and select **Upload** from the drop-down list.

   The TSV file will be downloaded using your browser's settings. By default, the file name is event-export-<date>_<time>.tsv.

The file is saved based on your web browser's settings.

Configuring the table of events

Responses to user SQL queries are presented as a table in the **Events** section. The fields selected in the custom query appear at the end of the table, after the default columns. This table can be updated.

The following columns are displayed in the events table by default:

- **TenantID**.
- **Timestamp**.
- **Name**.
- **DeviceProduct**.
- **DeviceVendor**.
- **DestinationAddress**.
- **DestinationUserName**.

In KUMA, you can customize the displayed set of event fields and their display order. The selected configuration can be saved to a preset.

When using SQL queries with data grouping and aggregation for filtering events, statistics are not available and the order of displayed columns depends on the specific SQL query.

In the events table, in the event details area, in the alert window, and in the widgets, the names of assets, accounts, and services are displayed instead of the IDs as the values of the SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID, and ServiceID fields. When exporting events to a file, the IDs are saved, but columns with names are added to the file. The IDs are also displayed when you point the mouse over the names of assets, accounts, or services.

Searching for fields with IDs is only possible using IDs.

To configure the fields displayed in the events table:

1. Click the ⚙ icon in the top right corner of the events table.

   A window for selecting the event fields that should be displayed in the events table will be displayed.

2. Select the check boxes opposite the fields that you want to view in the table. You can search for relevant fields by using the **Search** field.

   You can configure the table to display any event field from the KUMA event data model and the extended event schema. The **Timestamp** and **Name** parameters are always displayed in the table. Click the **Default** button to display only default event parameters in the events table.

   When you select a check box, the events table is updated and a new column is added. When a check box is cleared, the column disappears.

You can also remove columns from the events table by clicking the column title and selecting **Hide column** from the drop-down list.

3. If necessary, change the display order of the columns by dragging the column headers in the event tables.

4. If you want to sort the events by a specific column, click its title and in the drop-down list select one of the available options: **Ascending** or **Descending**.

The selected event fields will be displayed as columns in the table of the **Events** section in the order you specified.

The list of selected fields is stored locally in your browser settings. To make column display settings identical across different browsers or devices, we recommend using presets.

Refreshing events table

You can update the displayed event selection with the most recent entries by refreshing the web browser page. You can also refresh the events table automatically and set the frequency of updates. Automatic refresh is disabled by default.

To enable automatic refresh,

Select a refresh rate from the drop-down list in the upper-right part of the **Events** section:

- **5 seconds**
- **15 seconds**
- **30 seconds**
- **1 minute**
- **5 minutes**
- **15 minutes**

The events table now refreshes automatically.

To disable automatic refresh:

In the drop-down list of refresh rates in the upper-right part of the **Events** section, select **No refresh**.

Getting events table statistics

You can get statistics for the current events selection displayed in the events table. The selected events depend on the filter settings.

To obtain statistics:

Select **Statistics** from the ••• drop-down list in the upper-right corner of the events table, or click on any value in the events table and select **Statistics** from the opened context menu.

The **Statistics** details area appears with the list of parameters from the current event selection. The numbers near each parameter indicate the number of events with that parameter in the selection. If a parameter is expanded, you can also see its five most frequently occurring values. You can find relevant parameters by using the **Search fields** field.

In a high availability configuration, for all event fields that contain the FQDN of the Core, the **Statistics** section displays **core** instead of the FQDN.

The **Statistics** window allows you to modify the events filter.

When using SQL queries with data grouping and aggregation for filtering events, statistics are not available.

Viewing correlation event details

You can view the details of a correlation event in the **Correlation event details** window.

To view information about a correlation event:

1. In the **Events** section of the KUMA web interface, click a correlation event.

   You can use filters to find correlation events by assigning the `correlated` value to the `Type` parameter.

   The details area of the selected event will open.

2. Click the **Detailed view** button.

   The correlation event window will open. The event name is displayed in the upper left corner of the window.

You can also navigate to the correlation event window from the the **Related events** section of the alert information window. In this case, you can go back to the alert information window by clicking the link in the upper part of the window. Otherwise, KUMA does not display the link to an alert.

The **Correlation event details** section of the correlation event window contains the following data:

- **Correlation event severity**—the severity of the correlation event.
- **Correlation rule**—the name of the correlation rule that triggered the creation of this correlation event. The rule name is represented as a link that can be used to open the settings of this correlation rule.
- **Correlation rule severity**—the severity of the correlation rule that triggered the correlation event.
- **Correlation rule ID**—the identifier of the correlation rule that triggered the creation of this correlation event.
- **Tenant**—the name of the tenant that owns the correlation event.

The **Related events** section of the correlation event window contains the table of events related to the correlation event. These are base events that actually triggered the creation of the correlation event. When an event is selected, the details area opens in the right part of the web interface window.

The **Find in events** link to the right of the section header is used for alert investigation.

The **Related endpoints** section of the correlation event window contains the table of hosts related to the correlation event. This information comes from the base events related to the correlation event. Clicking the name of the asset opens the **Asset details** window.

The **Related users** section of the correlation event window contains the table of users related to the correlation event. This information comes from the base events related to the correlation event.

Generating an SQL query using KUMA SQL functions

KUMA's SQL functions allow using the attributes of assets and accounts in search queries to filter events, generate reports and widgets (graph type: **Table**). You can enrich events with data from dictionaries, tables, assets, and accounts using the following sets of functions:

- The enrich function set. Allows enriching query results with fields of the asset or account, values from a dictionary of the **Dictionary** type or a dictionary of the **Table** type. The `enrich` function set includes the following functions:
  - `enrich_assets`;
  - `enrich_accounts`;
  - `enrich_table`;
  - `enrich_dictionary`.
- The lookup function set. Allows adding conditions for assets and accounts to the search query. The `lookup` function set includes the following functions:
  - `lookup_assets`;
  - `lookup_accounts`;
  - `lookup_assets_category`.

> The maximum number of events per query is 10,000.

Using the 'enrich' function set in SQL queries

The `enrich` function set (see the table below) is used in the `SELECT` clause of an SQL query to enrich the results.

When using this set of functions, you cannot group events by enriched fields.

Widgets and reports enriched by the functions must be owned by no more than one tenant.

The values of asset fields that are specified in SQL queries are case-sensitive.

Description of the 'enrich' set of functions

Function	Event field	Asset field	Description
enrich_assets	DeviceAssetID DestinationAssetID SourceAssetID	name os osBuild ipAddress macAddress fqdn source software cii ramSize kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart kscStatusMask kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus lastVisible aistatus aiscore	Enriches the query result with asset fields based on the ID specified passed to the function. Example enrich_assets(DeviceAssetID, name)

Function	Event field	Asset field	Description

`enrich_accounts`	`SourceAccountID`
	`DestinationAccountID`
		`name`
		`guid`
		`domain`
		`cn`
		`dn`
		`employee_id`
		`email`
		`mail_nickname`
		`mobile`
		`sid`
		`sam_name`
		`telephone_number`
		`principal_name`
		`sn`
		`type`
		`title`
		`division`
		`department`
		`manager`
		`location`
		`company`
		`street_address`
		`physical_delivery_office_name`
		`uac`
			Enriches the query result with account fields based on the ID specified passed to the function.
			Example
			`enrich_account(SourceAccountID, name)`
			This function is available only for tenants that have LDAP enrichment enabled.

`enrich_table`	Any	–	Enriches the query result with values from a dictionary of the **Table** type based on event fields in the response from the ClickHouse cluster.
			Example
			`enrich_table('Main/some-table', [DeviceProduct], 'value')`
			Only one column of the table can be the key, but the record key can be a compound key.
			Example
			`enrich_table('Main/Dictionary', [BytesOut|BytesIn], 'value2')`
			The `enrich_table` function returns only one column of the table. If you need to call more columns, call the function again specifying the relevant fields.

`enrich_dictionary`	Any	—	Enriches the query result with values from a dictionary of the **Dictionary** type based on event fields in the response from the ClickHouse cluster.
			Example 1
			`enrich_dictionary('Main/some-dict', [SourceAddress]`
			Example 2
			`enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress])`
			You can view the path to the dictionary in the **Resources** → **Dictionaries** section.

You can specify an `enrich` function when manually creating SQL queries.

Example queries with an `enrich` function

All events of the `events` table with the `Name` and `Message` fields, as well as the `macAddress` and `osBuild` asset fields to enrich the result with asset data. The number of rows that can be displayed in the table is 250.

```
SELECT Name,
Message,
   enrich_assets(DeviceAssetID, macAddress),
   enrich_assets(DeviceAssetID, osBuild)
FROM `events`
WHERE DeviceAssetID != ''
LIMIT 250
```

All events of the `events` table with event fields `SourceUserName` and `SourceAddress`, as well as values of the `mobile` field to enrich the result with account data. The number of rows that can be displayed in the table is 10.

```
SELECT SourceUserName,
SourceAddress,
   enrich_accounts(SourceAccountID, mobile) as mobile
FROM `events`
WHERE SourceAccountID != ''
LIMIT 10
```

All events in the `events` table with `DeviceProduct` event fields with values from the **Main/[OOTB] Linux. Auditd record types**. Sorted by **Timestamp** in descending order. The number of rows that can be displayed in the table is 1000.

```
SELECT DeviceProduct,
   enrich_table('Main/[OOTB] Linux. Auditd record types', [DeviceProduct], 'Description') as HTTP
FROM `events` WHERE Type!=4
LIMIT 1000
```

All events in the `events` table with `DeviceAction` event fields with values from the **Main/[OOTB] KEDR** dictionary. The number of rows that can be displayed in the table is 255.

```
SELECT DeviceAction,
   enrich_dictionary('Main/[OOTB] KEDR. AccountType', [BytesOut]) as accountType
FROM `events` WHERE Type!=4
LIMIT 255
```

Using the 'lookup' function set in SQL queries

The `lookup` function set (see the table below) is used in the `WHERE` clause of an SQL query to add conditions for assets and accounts to the search query.

In queries containing a `lookup` function, KUMA automatically adds the `*ID` field to the `SELECT` clause, which field is used in the `lookup` function in the query. For example, in a query containing the `lookup_assets(DeviceAssetID, osBuild, '=', '19045.000000')` function a `DeviceAssetID` field is added to the `SELECT` clause.

> In queries containing the `lookup` function, we recommend specifying the list of fields to be returned in the `SELECT` clause. We do not recommend using * in the `SELECT` clause. This returns all available fields, which can make the query take significantly longer to be processed.

Function type	Event field	Asset field	Operator	Description
lookup_assets	DeviceAssetID SourceAssetID DestinationAssetID	name os osBuild source cii ramSize kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus aistatus aiscore	=	Allows you to add conditions t result for assets whose field v value specified in the query. For values that are number, yo string with the required numbe For example: lookup_assets(DeviceAss '=', '19045.000000') lookup_assets(DeviceAss '=', '3241234234')
		kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart lastVisible ramSize aiscore	< > <= >=	Allows you to add conditions f field values that are: • Less than the value speci • Greater than the value sp query • Less than or equal to the the query • Greater than or equal to t specified in the query For values that are number, yo string with the required numbe For example: lookup_assets(DeviceAss '>', '50') Date values can be specified i formats: • Number of seconds: lookup_assets(Device lastVisible, '>', '1 • Number of milliseconds: lookup_assets(Device lastVisible, '<', '1725971837834') • Number of days: lookup_assets(Device lastVisible, '<', 'n
		name os osBuild fqdn software	like	Allows you to add conditions t result for assets whose field v 'like' expression specified in th For more information about th please refer to the SQL Langu Expressions reference. lookup_assets(Destinati name, 'like','test.compa
		ipAddress macAddress fqdn software kscStatusMask	in	Allows you to add to the resul whose values match the value query. For example: lookup_assets(DeviceAss 'in', ['test_fqdn1.compa 'test_fqdn2.company.ru']

Function type	Event field	Asset field	Operator	Description
		`ipAddress`	`insubnet`	Allows you to add conditions f addresses in the specified sub address is specified in CIDR fo For example: `lookup_assets(DeviceAss ipAddress, 'insubnet',`
		`ipAddress`	`inrange`	Allows you to add conditions f addresses in the specified ran The first IP address specified i start IP address, and the seco address. For example: `lookup_assets(DeviceAss ipAddress, 'inrange', [ '192.168.1.184'])` The query filters assets with IP range from 192.168.1.1 to 192.168

Function type	Event field	Asset field	Operator	Description
lookup_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn title division department manager location company street_address physical_delivery_office_name uac	=	Allows you to add conditions t result for accounts whose fiel the value specified in the quer For values that are number, yo string with the required numbe For example: lookup_accounts(SourceA employee_id, '=', '1545
		name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name	like	Allows you to add conditions t result for accounts whose fiel the 'like' expression specified i For more information about th please refer to the SQL Langu Expressions reference. lookup_accounts(Destina name, 'like', '_ccount1

Function type	Event field	Asset field	Operator	Description

`lookup_assets_category`	`DeviceAssetID`
	`SourceAssetID`
	`DestinationAssetID`
		–	–	Finds all events that have assc the specified folder.
				For example:
				`lookup_assets_category( ['Main/Business Impact']`
				where `Main` is the name of th `Business Impact` is the nar

Example SQL queries with a lookup function

You can specify a `lookup` function when manually creating SQL queries. Example queries with a `lookup` function

- All events of the 'events' table with the `TenantID` and `DeviceProduct` event fields, as well as the `fqdn` asset field, whose value contains the win10 substring. The number of rows that can be displayed in the table is 250.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets(DeviceAssetID, fqdn, 'match', 'win10')
LIMIT 250
```
- All events in the 'events' table, with the `TenantID` and `DeviceProduct` event fields, and with values of `the EmployeeID` field, whose value is `15452.` The number of rows that can be displayed in the table is 10.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE SourceAccountID != ''
AND lookup_accounts(SourceAccountID, employee_id, '=', '15452')
LIMIT 10
```
- All events of the 'events' table with the `TenantID` and `DeviceProduct` event fields, with the folder in which the asset is located. The number of rows that can be displayed in the table is 100.
```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets_category(DeviceAssetID, ['Main/Business Impact'])
LIMIT 100
```

Data collection and analysis rules

Data mining rules are used for detecting incidents by analyzing events saved in the KUMA database.

Unlike streaming correlation and retrospective scan, data collection and analysis rules involve the preprocessing of data using SQL queries (including additional calculations, grouping and aggregation using SQL) and running regularly on a schedule. With correctly configured data mining rules, the SIEM can help you detect advanced threats.

To manage the section, you need one of the following roles: General administrator, Tenant administrator, Tier 1 analyst, Tier 2 analyst.

When creating or editing data collection and analysis rules, you need to specify the settings listed in the table below.

Settings of data collection and analysis rules

Setting	Description
Name	Required setting. Unique name of the resource. Must contain 1 to 128 Unicode characters.
Tenant	Required setting. The name of the tenant that owns the resource. If you have access to only one tenant, this field is filled in automatically. If you have access to multiple tenants, the name of the first tenant from your list of available tenants is inserted. You can select any tenant from this list.

SQL	Required setting.
	The SQL query must contain an aggregation function with a LIMIT and/or a data grouping with a LIMIT.
	You must use a LIMIT value between 1 and 10,000.
	Examples of SQL queries
	• A query containing only an aggregation function:
	`SELECT count(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	• A query containing only data grouping:
	`SELECT SourceAddress, DeviceCustomFloatingPoint1 FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• A query containing an aggregation function and data grouping:
	`SELECT SourceAddress, sum(DeviceCustomFloatingPoint1) FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• A query containing an expression using aggregation functions:
	`SELECT stddevPop(DeviceCustomFloatingPoint1) + avg(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	You can also use SQL function sets: `enrich` and `lookup`.

SQL query execution frequency	Required setting. The interval for executing the SQL query. You can specify the interval in minutes, hours, and days. The minimum interval is 1 minute. The default timeout of the SQL query is equal to the interval that you specify in this field. If the execution of the SQL query takes longer than the timeout, an error occurs. In this case, we recommend increasing the interval. For example, if the interval is 1 minute, and the query takes 80 seconds to execute, we recommend setting the interval to at least 90 seconds.
Tags	Optional setting. Tags for resource search.
Depth	Optional setting. Expression for the lower bound of the interval for searching events in the database. To select a value from the list or to specify the depth as a relative interval, place the cursor in the field. For example, if you want to find all events from one hour ago to now, set the relative interval of `now-1h`.
Description	Optional setting. Description of data collection and analysis rules.
Mapping	Settings of the mapping the fields of an SQL query result to KUMA events: **Source field** is the field from the SQL query result that you want to convert into a KUMA event. **Event field** is the KUMA event field. You can select one of the values in the list by placing the mouse cursor in this field. **Label** is a unique custom label for event fields that begin with DeviceCustom*. You can add new table rows or delete table rows. To add a new table row, click **Add mapping**. To delete a row, select the check box next to the row and click the 🗑 button. If you do not want to fill in the fields manually, you can click the **Update mapping from SQL** button. The field mapping table is populated with the values of the SQL query fields, including aliases (if any). For example, if the value of an SQL query field is `SourceAddress` and this value is the same as the name of an event field, this value is inserted into in the **Event field** column in the field mapping table. Clicking the **Update mapping from SQL** button again does not refresh the table, and fields from the SQL query are added to it again.

You can create a data collection and analysis rule in one of the following ways:

- In the **Resources** → **Resources and services** → **Data collection and analysis rules** section.
- In the **Events** section.

*To create a data collection and analysis rule in the **Events** section:*

1. Create or generate an SQL query and click the button.

   A new browser tab for creating a data collection and analysis rule is opened in the browser with pre-filled **SQL query** and **Depth** fields. The field mapping table is also be populated automatically if you did not use an asterisk (*) in the SQL query.

2. Fill in the required fields.

   If necessary, you can change the value in the **SQL query execution frequency** field.

3. Save the settings.

The data collection and analysis rule is saved and is available in the **Resources and services** → **Data collection and analysis rules** section. For a data collection and analysis rule to run, you must create a scheduler for it.

Managing data collection and analysis rules

You can create, copy, edit, and delete data mining rules.

Creating a data mining rule

To create a data mining rule:

1. In the web interface, open the **Resources** → **Data mining rules** and click the **Create** button.

   This opens the data mining rule creation pane.

2. Specify the following rule settings:

   a. Enter a resource name in the **Name** field. The resource name must be unique within the selected tenant.

   b. In the **Tenant** drop-down list, select the tenant to which the data mining rule will belong.

   c. If necessary, add tags from the **Tags** drop-down list.

   d. Specify the period for the data mining requests.

   e. If necessary, set a lower bound for the data retrieval period.

   f. If necessary, enter an SQL query that must contain grouping (`GROUP BY`) or aggregation functions and a `LIMIT`. The `LIMIT` value is supported for the following number of records: from 1 to 10,000.

3. Under **Mapping**, configure the mapping of raw event fields to event fields: To do so:

   a. Click **Add mapping**.

      You can add multiple table rows or delete table rows. To delete a table row, select the check box next to it and click the **Delete** button.

   b. In the **Source field** column, specify the name of the raw event field that you want to map to the KUMA event field.

   c. In the **Event field** column, select a KUMA event field from the drop-down list.

4. Click **Create**.

The data mining rule is created and becomes available for use in resources.

You can also create a data mining rule based on the SQL query that you created in the **Events** section. To do this, in the menu under the query field (⋮), select **Create data mining rule**. The generated SQL query is automatically copied in the data mining rule creation pane.

Copying a data mining rule

To copy a data mining rule:

1. In the web interface, open the **Resources** → **Data mining rules** section and select the check box next to the rule that you want to copy.

2. Click **Duplicate**.

   This will display the number of selected rules in the lower part of the table.

   A pane with the settings of the data mining rule that you have selected for copying is opened on the right side of the screen.

   The **Name** field displays `<name of the selected rule> - copy`.

3. Change the settings as needed (see the instructions for creating a data mining rule).

4. Click **Save**.

A copy of the data mining rule is created.

Settings of data mining rules

To edit a data mining rule:

1. In the web interface, open the **Resources** → **Data mining rules** section and click the rule that you want to edit.

   This opens the pane with settings of the selected data mining rule.

2. Change the settings as needed (see the instructions for creating a data mining rule).

3. Do one of the following:

   - Click **Save** to save your changes.

   - Click **Save with comment**, and in the window that opens add a comment that describes your changes. The changes are saved and the comment will be added to the created version of the data mining rule.

The data mining rule is updated.

Deleting data mining rules.

To delete a data mining rule:

1. In the web interface, open the **Resources** → **Data mining rules** section and select the check box next to the rule that you want to delete.

   The number of selected resources is displayed in the lower part of the table.

2. Click **Delete**.

3. In the window that opens, confirm the deletion.

The data mining rule and all its saved versions are deleted.

Configuring the scheduler for a data collection and analysis rule

For a data collection and analysis rule to run, you must create a scheduler for it.

The scheduler makes SQL queries to specified storage partitions with the interval and search depth configured in the rule, and then converts the SQL query results into base events, which it then sends to the correlator.

> SQL query results converted to base events are not stored in the storage.

For the scheduler to work correctly, you must configure the link between the data collection and analysis rule, the storage, and the correlators in the **Resources** → **Data collection and analysis** section.

To manage this section, you need one of the following roles: General administrator, Tenant administrator, Tier 2 analyst, Read shared resources, Manage shared resources.

The schedulers are arranged in the table by the date of their last launch. You can sort the data in columns in ascending or descending order by clicking the down arrow (⌄) icon in the column heading.

Available columns of the table of schedulers:

- **Rule Name** is the name of the data collection and analysis rule for which you created the scheduler.
- **Tenant name** is the name of the tenant to which the data collection and analysis rule belongs.
- **Status** is the status of the scheduler. The following values are possible:
  - **Enabled** means the scheduler is running, and the data collection and analysis rule will be started in accordance with the specified schedule.
  - **Disabled** means the scheduler is not running.

    This is the default status of a newly created scheduler. For the scheduler to run, it must be **Enabled**.
- **The scheduler finished at** is the last time the scheduler's data collection and analysis rule was started.

- **Rule run status** is the status with which the scheduler has finished. The following values are possible:
  - **Ok** means the scheduler finished without errors, the rule was started.
  - **Unknown** means the scheduler was **Enabled** and its status is currently unknown. The **Unknown** status is displayed if you have linked storages and correlators on the corresponding tabs and **Enabled** the scheduler, but have not yet started it.
  - **Stopped** means the scheduler is stopped, the rule is not running.
  - **Error** means the scheduler has finished, and the rule was completed with an error.
- **Recent Error** lists errors (if any) that occurred during the execution of the data collection and analysis rule.

> Failure to send events to the configured correlator does not constitute an error.

You can use the toolbar in the upper part of the table to **perform actions on schedulers**.

- Add a new scheduler. Click the **Add** button, and in the displayed window, select the check boxes next to the names of the data collection and analysis rules for which you want to create a scheduler.

  > In this window, you can select only data collection and analysis rules that have been created previously. You cannot create a new rule.

- Remove a scheduler. In the table of schedulers, select the check boxes next to the schedulers that you want to delete and click the **Delete** button. The scheduler and links are removed. The data collection and analysis rule is not removed.
- Enable a scheduler. In the table of schedulers, select the check boxes next to the schedulers that you want to enable and click the **Enable according to schedule** button. The data collection and analysis rule for which this scheduler was created will be executed in accordance with the schedule configured in the settings of this rule.
- Disable a scheduler. In the table of schedulers, select the check boxes next to the schedulers that you want to disable and click the **Disable** button. The data collection and analysis rule is paused, but the scheduler itself and the links are not deleted.
- Start the scheduler. In the schedulers table, select the check boxes next to the enabled schedulers and click the **Run now** button. This scheduler's data collection and analysis rule is executed immediately.

To edit the scheduler, click the corresponding line in the table.

Available scheduler settings for data collection and analysis rules are described below.

General tab

On this tab you can:

- Enable or disable the scheduler using a toggle switch.

  If the toggle switch is enabled, the data collection and analysis rule runs in accordance with the schedule configured in its settings.

- Edit the following settings of the data collection and analysis rule:
  - Name
  - Query interval
  - Depth
  - Sql
  - Description
  - Mapping

The Linked storages tab

In this tab you need to specify a storage for the scheduler to send SQL queries to.

To specify a storage:

1. Click the **Link** button in the toolbar.
2. This opens a window; in that window, specify the name of the storage to which you want to add the link, as well as the name of the section of the selected storage.

   > You can select only one storage, but multiple sections of that storage.

3. Click **Add**.

   The link is created and displayed in the table on the **Storage bindings** tab.

If necessary, you can remove the links by selecting the check boxes in the relevant rows of the table and clicking the **Unbind selected** button.

The Linked correlators tab

On this tab, you must add correlators for handling base events.

To add a correlator:

1. Click the **Link** button in the toolbar.
2. This opens a window; in that window, hover over the **Correlator** field.

3. In the displayed list of correlators, select check boxes next to the correlators you want to add.

4. Click **Add**.

   The correlators are added and displayed in the table on the **Correlator bindings** tab.

If necessary, you can remove the correlators by selecting the check boxes in the relevant rows of the table and clicking the **Unbind selected** button.

You can also view the result of the scheduler in the Core log; to do so, you must first configure the **Debug** mode in Core settings. To download the log, select the **Resources** → **Active services** in KUMA, then select the Core service and click the **Log** button.

Log records with scheduler results have the `datamining scheduler` prefix.

Analyzing network traffic volume

When receiving events in the NetFlow format, it becomes necessary to analyze the volume of network traffic between hosts. You can use correlation rules to count traffic between hosts, but the large numbers of accesses to active lists makes this approach inefficient.

To analyze the volume of network traffic, we recommend using the data mining rules, which allow getting traffic data and identifying patterns in the mass of events in the NetFlow format.

You can follow this scenario to create a data mining rule for counting network traffic. For each stage, there are links to instructions for performing the necessary steps and additional materials for review.

1 Creating a data mining rule

Create a data mining rule for analyzing traffic between hosts with the following SQL query parameters:

- Grouping (`GROUP BY`) by `SourceAddress` and `DestinationAddress`.
- Aggregation by fields (for example, `SUM(BytesIn + BytesOut) AS TotalTraffic`).
- Set the period for the data mining rule to one hour.
- Set the search query depth to one hour.

  If you want to analyze network traffic for a different period, you need to specify this period instead.
- Set the maximum number of events for analysis (`LIMIT`) to 10,000.

Under **Mapping**, also specify the settings for the mapping of the SQL query result fields to KUMA events. You can do this by clicking the **Update mapping from SQL** button.

> When using a parameter for an aggregated expression (`AS`), you need to specify the value manually. For example, for the `TotalTraffic` parameter, in the **Source field** field in the **Event field** , specify `DeviceCustomNumber1`.

Example of SQL search query

```
SELECT SourceAddress, DestinationAddress, SUM(BytesIn + BytesOut) AS TotalTraffic
FROM 'events'
GROUP BY SourceAddress, DestinationAddress
LIMIT 10000
```

❷ Linking a data mining rule to services

After creating a data mining rule:

1. Add the rule to the scheduler by linking a storage and a correlator to the data mining rule.
2. Enable the toggle switch to allow using of the created rule for analyzing traffic between hosts.

   The toggle switch is turned off by default.

❸ Creating a correlation rule

After linking the data mining rule, create a correlation rule to be used in the linked correlator. When creating the rule, consider the following:

- On the **General** tab, in the **Identical fields** drop-down list, select all the values used in the data mining rule (`SourceAddress, DestinationAddress, DeviceCustomNumber1`).
- The value of the **Rate limit** setting must correspond to the maximum number of events to be analyzed by the data mining rule.
- On the **Selectors** tab in the filter builder, specify a value in bytes for the maximum traffic volume per the selected time unit. For example, if you want to set a traffic volume of 1 GB, specify the setting as follows:

  ```
  DeviceCustomNumber1 ≥ 1073741824
  ```

- On the **Actions** tab, select the **Output** check box.

KUMA Core accumulates event information in the solution and sends it to the correlator, where the correlation rule is applied. If the traffic exceeds the specified value per hour, the solution creates an alert.

Retroscan

In normal mode, the correlator handles only events coming from collectors in real time. **Retrospective scan** allows you to apply correlation rules to past events if you want to debug correlation rules or analyze data.

To test a correlation rule, you do not need to replay the incident in real time. Instead, you can run the correlation rule in **Retrospective scan** mode to process the existing events which include the required incident.

You can use a search query to define a list of events for retrospective scan, as well as specify a search period and the storage that you want to search for events. You can configure a task to have alerts generated and response rules applied during the retrospective scan of events.

To run a retrospective scan:

1. In the **Events** section of the KUMA web interface, create the required event selection:

   - Select the storage.

     > Before running a retrospective scan, make sure that the correct clusters and spaces are selected.

   - Configure search expression using the constructor or search query.

     > Before running a retrospective scan, make sure that the correct expression is specified in the SQL query field.

   - Set a period as needed.

     > Before running a retrospective scan, make sure that the correct period is selected in the period field.

2. Open the ··· drop-down list and choose **Retrospective scan**.
   The retrospective scan window opens.

3. In the **Correlator** drop-down list, select the Correlator to feed selected events to.

   > Before running a retrospective scan, check the number of events found by the SQL query. This information is displayed under **Show timeline** → **Total**. If the **LIMIT** parameter value is not specified in the SQL query, all events for the period are sent to the correlator and the task takes longer to complete. If a relative period is set (for example, *now-1h*), new events may be produced by the start of the retrospective scan; such events are also sent to the correlator. If the correlator is not installed in the Main tenant, it can only receive events of its own tenant.

4. In the **Correlation rules** drop-down list, select the Correlation rules that must be used when processing events. If no rules are selected at this step, the scan is performed with all correlation rules applied.

5. In the **EPS limit** field, specify the maximum EPS to be used for a retrospective scan. The specified value sets the maximum load when performing a retrospective scan. The default setting is 0, which means that no EPS limit is applied to a retrospective scan.

   Negative EPS values are not allowed.

6. If you want responses to be executed when processing events, turn on the **Execute responses** toggle switch.

7. If you want alerts to be generated during event processing, turn on the **Create alerts** toggle switch.

8. Click the **Create task** button.

   The retrospective scan task is created and displayed in the **Task manager** section.

To view scan results, in the **Task manager** section of the KUMA web interface, click the task you created and in the drop-down list, select **Go to Events**.

Retrospective scan results only show the generated correlation events.
The start of the period in retrospective scan results is displayed as <date and time of the task creation>, and the end of the period is shown as <date and time of task creation + one hour> (or the current time if one hour has not yet elapsed since the task creation).
If there are no events in the retrospective scan results, it means that the correlator was not triggered by events from the SQL selection that were sent to it.

A new browser tab is opened, containing events that were processed during the retrospective scan, as well as aggregated and correlation events created during event processing. Correlation events generated by the retrospective scan have an additional ReplayID field that stores a unique ID of the retrospective scan. An analyst can restart the retroscan from the context menu of the task. New correlation events will have a different ReplayID.

Depending on your browser settings, you may be prompted to confirm the opening of the retrospective scan results tab. For more details, please refer to the documentation for your specific browser.

Events processed by retrospective scan are not enriched with data from CyberTrace or the Kaspersky Threat Intelligence Portal.

Active lists are updated during retrospective scan.

Retrospective scan cannot be performed based on SQL queries that contain arithmetic expressions or only aggregation fields. You can retrospectively scan groups of events obtained using a grouping SQL query only after the processing of the query has finished. To do this, first run SQL query with data grouping and get a list of event groups, and then run a retrospective scan on one of the groups.

Event route tracing

To find out which connection the events were received from, you can use the **Track event route** setting. You may need to trace the route of an event when multiple agents send events to the same collector, for example, in a large infrastructure where agents are installed on dedicated WEC servers and multiple agents send events to the same collector. The event route information can be useful for troubleshooting event routing.

For the **Track event route** toggle switch to become available, you must specify at least one **internal** destination in the agent. Also, to trace event routes, a connector of the **internal** type must be specified in the collector that is receiving events from the agent. After configuring and saving the agent, information about the agent's route is added to the **S.KL_EventRoute** field of the extended event schema.

The **S.KL_EventRoute** field is displayed only for new events that are received by the collector after enabling the **Track event route** setting. Other services through which the event passes, including the collector, correlator (only correlation rules of the 'simple' type), and router, parse the **S.KL_EventRoute** field, and, if the field is not empty, add their own information to the field when they process the event.

If the event passes through multiple hosts on its way from the sender to the agent, the address of the last host that established a connection with the agent is saved in the **S.KL_EventRoute** field. If there is a proxy server between the sender and the agent, the address of this proxy server is written to the field, and no separate proxy server configuration is required on the agent. The tcp/udp/http connectors pass the address of the host from which the event was received via the **internal** protocol to **S.KL_EventRoute**, and the WEC, WMI, and ETW agents specify the host name of the Windows server on which they are installed.

You can enable event route tracing in one of the following ways:

- Create a new agent, specify the **internal** destination in it and enable the **Track event route** option.

- In an existing agent, add a tab with a new connection and specify the **internal** destination on this tab. After you specify the **internal** destination, the **Track event route** option becomes available. Enable the **Track event route** toggle switch. After you save the agent settings, restart the agent to apply the changes. In this case, route tracing only affects the tab on which the **internal** destination is selected, not the entire agent.

- Unlink the automatically created agent from the collector to make the agent available for editing its settings, or duplicate the automatically created agent and proceed to configure the settings in the duplicate agent. After you specify an **internal** destination in an editable agent, the **Track event route** option becomes available. Enable the **Track event route** toggle switch. After you save the agent settings, restart the agent to apply the changes. In this case, route tracing only affects the tabs on which the **internal** destination is selected, not the entire agent.

The **Event tracking log** section appears in the event card, alert card and correlation event card. This section displays information from the **S.KL_EventRoute** field in a processed form. Service IDs are converted to service names and displayed as clickable links. Clicking a service name opens a new browser tab with the card of the service. If you rename the service, the name of the service also changes when the event is displayed in the card, both for new events and for events that have already been received and processed. If you delete a service in the **Active services** section, the **Event tracking log** section displays **Deleted** instead of the hyperlink. The rest of the route information is not deleted and is still displayed, including the connector type, FQDN, the value of the **SourceAddress** field, and other route parameters from the **S.KL_EventRoute** field. To view raw route information, you can add the **S.KL_EventRoute** column to the event table.

Using route information

You can use the 'Extract from JSON' function or other ClickHouse functions to get the parts of the route that you need for debugging. For more information about functions, please refer to the ClickHouse documentation: https://clickhouse.com/docs/en/sql-reference/functions/json-functions#jsonextractstringjson-indices-or-keys

The following table gives examples of queries.

Query example	Description
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'version') as version FROM `events` Where Type !=4 ORDER BY Timestamp DESC LIMIT 25`	This query displays events for which the version of the collector is displayed in the **version** column.
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') as connectorKind FROM `events` Where Type !=4 ORDER BY Timestamp DESC LIMIT 250`	This query displays events for which the type of the collector is displayed in the **connectorKind** column.
`SELECT *, simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') as connectorKind FROM `events` Where Type !=4 and simpleJSONExtractRaw(S.KL_EventRoute, 'connectorKind') != '"wec"' ORDER BY Timestamp DESC LIMIT 250`	This query displays events received from connectors of a type other than 'wec'.

If want to select by a different value from the **S.KL_EventRoute** field, you can look up the name of your parameter in the events table in the **Raw** column and use it in your query.

Categorization of events

Categorization allows you to use special tags (categories) to describe events of the same type coming from different sources. This helps to find events related to, for example, user authentication or command execution, and helps in writing correlation logic or displaying data in a dashboard or in reports. You can use the KUMA resource set to categorize certain types of events for specific types of event sources.

The following types of KUMA resources are used to categorize events:

- A dictionary with categories of events
- enrichment rules for supplementing events with additional information;
- A normalizer for creating an extended event schema field used in enrichment rules.

As part of categorization, the following attributes can be added to an event:

- Object
- Action
- Result
- Threat
- Source type

Additional attributes can be assigned to the event, which are saved in the SA.KL_EventCategory extended event schema field.

Descriptions of the possible values of the attributes used for categorizing events are provided in tables: *Object attribute, Action attribute, Result attribute, Threat attribute, Source type attribute*.

To customize the categorization of events on a collector:

1. Import the [OOTB] Event Categorization package from the KUMA repository.
2. In the collector, apply an event enrichment rule at the **Event enrichment** step.

You can apply the enrichment rule when creating a new collector or for an existing collector. The rule that you need to apply depends on the event source. You can select a rule from the *Categorization rules by event source* table.

> Event categorization works only when using Kaspersky normalizers.

3. In the KUMA web interface, select the **Resources** → **Active services** section.

4. Select the check box next to the modified collector and click the **Update configuration** button.

The enrichment rule is applied, and the categorization of events is performed.

Categorization rules by event source

System name	Normalizer name	Enrichment rule name
Microsoft, OS event logs	[OOTB] Microsoft Products for KUMA 3	[OOTB] Event categorization. Microsoft Products
Microsoft Sysmon	[OOTB] Microsoft Products for KUMA 3	[OOTB] Event categorization. Microsoft Products
Auditd	[OOTB] Linux auditd syslog for KUMA 3.2	[OOTB] Event categorization. Auditd
Kaspersky Security Center	[OOTB] KSC from SQL	[OOTB] Event categorization. Kaspersky Security Center
Kaspersky Security for Linux Mail Server	[OOTB] KLMS syslog CEF	[OOTB] Event categorization. Kaspersky Security for Linux Mail Server
Kaspersky IoT Secure Gateway	[OOTB] Kaspersky KISG syslog	[OOTB] Event categorization. Kaspersky IoT Secure Gateway
Kaspersky Container Security	[OOTB] Syslog-CEF	[OOTB] Event categorization. Kaspersky Container Security
Kaspersky Industrial CyberSecurity for Networks	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	[OOTB] Event categorization. Kaspersky Industrial CyberSecurity for Networks
Kaspersky Web Traffic Security	[OOTB] KWTS syslog CEF	[OOTB] Event categorization. Kaspersky Web Traffic Security
Kaspersky Mail Security Gateway	[OOTB] KSMG syslog CEF	[OOTB] Event categorization. Kaspersky Mail Security Gateway

Object attribute

Value of the Object attribute	Description
account	Accounts
configuration	Settings
connection	Network connection
container	Containers
data	Data or tables in the database
dns	DNS queries
email	Email
file	Files
group	Groups
host	Host
http	WEB requests
image	DLLs and drivers
malware	Malicious object
permission	Rights and privileges

Value of the Object attribute	Description
process	Process
registry	Registry keys
service	Services and daemons
task	Tasks
VM	Virtual machine
device	Token, USB device, attached device
certificate	Certificate

Action attribute

Value of the Action attribute	Description
access	Request or grant access to an object
add	Create or add
authentication	Authenticate
block	Block, prevent
delete	Delete
detect	Detect or quarantine
end	End of the process
info	Informational event about the object
load	Load object
modify	Modify settings or state of the object
read	Read
receive	Receive
request	Query
send	Send
start	Start of the process
write	Write

Result attribute

Value of the Result attribute	Description
error	Error
failure	Failure
success	Success

Threat attribute

Value of the Threat attribute	Description
malware	Malicious object in the file system
vulnerability	Vulnerability exploits
attack	Attack
ddos	Indicators of a DDoS attack
phishing	Indicators of phishing
c2	Command and Control
discovery	Reconnaissance
policy violation	Violation of security policies

Value of the Threat attribute	Description
tools	Suspicious tools used
escalation	Privilege escalation

Source type attribute

Value of the Source type attribute	Description
application	Application-level events: logins, configuration changes, errors, and so on.
AV	Events received from anti-virus protection systems.
database	Events from databases related to data manipulation.
IDS	Events from traffic analyzers and network protection tools.
network	Events containing information about network connections coming from firewalls; also events from Netflow, Jflow, and so on.
OS	Events from the operating system, such as Windows, Linux, Cisco IOS, HP-UX, and so on. Standard operating system tools or EDR can be the event provider.
vpn	VPN session events.
web	Events coming from WEB applications and Proxy. Application-level HTTP connection events.
container	Events providing information about the operation of containers.

Granular access to events

In KUMA, users with different rights can have granular access to events. Access to events is controlled at the level of storage spaces.

You can assign spaces to users in the **Access to spaces** section or directly in a user's card. An event contains a tenant ID and a space ID, therefore the user needs rights to the corresponding tenant and space to have access to the event.

Consider the following features of displaying storages:

- If a storage is not listed in the **Active services** section, the storage and its spaces are not displayed in the list of spaces of the set.
- If the storage service was stopped using the `systemctl stop kuma-<storage ID>` command, the storage and its spaces are not displayed in the list of spaces of the set.
- If the storage was started and then deleted using the `uninstall` command, the storage and its spaces remain in the list of spaces of the set.

In the list of events, you can add the **SpaceID** field to the table, which will display the name of the space. The space of audit events is displayed as KUMA Audit. KUMA Default is the space inside each storage, where all events go if the storage does not have configured spaces or if the event does not match the conditions of the existing spaces.

When you export the list of events to a TSV file, the space ID and name are displayed for spaces.

To differentiate access:

1. Assign appropriate roles to users.

2. Configure the space sets.

   You can create, edit, or delete space sets. These actions result in audit events.

3. Configure the access rights of the space set: you can grant or revoke access rights of selected users.

You can also view various scenarios for using granular access to events.

Managing sets of spaces

In KUMA, it is possible to grant granular access to events for users with different rights. Access to events is controlled at the level of storage spaces.

Creating a space set

To create a space set:

1. In the KUMA web console, go to the **Settings** → **Access** → **Access to spaces** section.

2. In the opened window, click the **Add** button.

3. In the **Create space sets** window, configure the following:

   a. In the **Name** field, specify the space set name. You can use up to 128 Unicode characters.

   b. In the **Spaces** drop-down list, select the spaces that you want to include in the set by selecting the check box next to the space name. To remove a space from the set, clear the check box.

   c. If you want the default space set to be available to all users that do not have any of the sets assigned, select the **Make default** check box.

      This makes the created set the default set. In the list of space sets, it is marked as the default set: in the **Default** column, it has **Yes**.

      There can be only one default set. If you select **Make default** check box in the settings of a different set and save the settings, the default set is reassigned.

4. Click **Create**.

The space set is created and displayed in the list of spaces. After the space set is created, an audit event is generated in KUMA.

Then you need to grant users access rights to the created space set.

Editing a space set

To edit a space set:

1. In the KUMA web console, go to the **Settings** → **Access** → **Access to spaces** section.
2. In the opened window, click a set of spaces.
3. In the **Edit space sets** window, configure the following:
   a. In the **Name** field, specify the space set name. You can use up to 128 Unicode characters.
   b. In the **Spaces** drop-down list, select the spaces that you want to include in the set by selecting the check box next to the space name. To remove a space from the set, clear the check box.
   c. If you want the default space set to be available to all users that do not have any of the sets assigned, select the **Make default** check box.

      This makes the set the default set when you save the changes. In the list of space sets, it is marked as the default set: in the **Default** column, it has **Yes**.

      There can be only one default set. If you select **Make default** check box in the settings of a different set and save the settings, the default set is reassigned.
4. Click **Save**.

The space set is saved and displayed in the list of spaces.

The edited set of spaces is accessible to all users who had access to the original space set. You can control access to the edited space set and grant or revoke access permissions using the **Access control** button.

Deleting a space set

To delete a space set:

1. In the KUMA web console, go to the **Settings** → **Access** → **Access to spaces** section.
2. In the **Access to spaces** window, select the check box next to the relevant space set.

   If you want to delete all space sets, select the **Select all** check box in the upper left part of the list and click **Delete**.

   > You cannot delete the default space set and the 'All spaces' space set.
3. Click **Delete**.

   The space set is deleted and removed from the list of spaces. After the space set is deleted, an audit event is generated in KUMA.

If a user had access only to the deleted space set and did not have access to any other sets, such a user automatically gets access rights to the default space set.

Grant access to a space set

To grant access to a space set

1. In the KUMA web console, go to the **Settings** → **Access** → **Access to spaces** section.
2. Select a set of spaces in the list by selecting the check box next to it, then click the **Access control** button on the toolbar.
3. This opens the **Users** window; in that window, click **Add users**.
4. In the list in the **Add users** window, select users to which you want to grant access to the space set and click **Add**.

   If you want to grant access to the selected space set to all users, select the check box in the upper left corner and select one of the following options: **Select all in page** or **Select all**, then click **Add**.

   This opens a confirmation window.
5. If you want to grant access to the listed users, click **Confirm** in the confirmation window.

The users now have access to the space set.

Revoke access to a space set

To revoke access to a space set

1. In the KUMA web console, go to the **Settings** → **Access to spaces** section.
2. Select a set of spaces in the list by selecting the check box next to it, then click the **Access control** button on the toolbar.
3. This opens the **Users** window; in that window, select users by selecting their check boxes, then click **Delete**.

   If you want to revoke access to the selected space set from all users, select the check box in the upper left corner and select one of the following options: **Select all in page** or **Select all**, then click **Delete**.

   This opens a confirmation window.
4. If you want to revoke access from the listed users, click **Confirm** in the confirmation window.

The users no longer have access to the space set.

If a user does not have access to any other space set, such a user automatically gets access to the default set.

Scenarios for using granular access to events

In KUMA, users with different rights can have granular access to events. This article provides examples of configuring granular access to events.

Access control for network core administrators and last-mile administrators

Purpose: KUMA collects events from network equipment. The telecommunications department has core network administrators and last-mile equipment administrators. A tenant named "telecom" has been created for access control, and events from network equipment are sent to it. However, this does not solve the issue of separating access rights for different administrators. Access rights must be configured to ensure that core network administrators have access to all events in the "telecom" tenant, while last-mile administrators have access only to events from last-mile equipment.

Action: the storage must be configured to ensure that events from network equipment are stored in different storage spaces. Then different users can be granted access to different spaces.

This scenario consists of the following stages:

1. **Creating storage spaces**

   In the "telecom" tenant storage, create two spaces:

   - For events from network core equipment.

     For example, name the space telecom_core.

   - For events from last-mile equipment.

     For example, name the space telecom_last_mile.

2. **Configuring space filters**

   Configure the filters of the created spaces so that only events from the network core go to the telecom_core space, and only events from the last-mile equipment go to the telecom_last_mile space.

3. **Assigning access rights to KUMA users**

   Configure access rights for spaces in user settings. For last-mile administrators, assign rights to the telecom_last_mile space only, and for network core administrators, specify All spaces.

Result: network core administrators have access to all events of the "telecom" tenant, and last-mile administrators have access only to events from the last-mile equipment.

Restricting access to spaces for all users

Goal: Some spaces in the installation must be inaccessible to some users. Current and new users must not have access to such spaces.

Action: The administrator creates a new set of spaces that includes the spaces to which all users must have access. Each space is specified as a tuple: clusterID, tenantID, spaceID. In this way, you can assemble a set of spaces from a finite number of spaces. After creating the set, the administrator makes this set the default set.

Result: For all users that do not have this space set explicitly specified, including new users, access to events is additionally restricted in accordance with the default space set. That is, such users have access to events in tenants in which the user has the right to view the list of events, and events in spaces that are included in the default set.

Allowing some users to view all events

Goal: KUMA has a default set in which only a finite number of spaces is explicitly specified. Also some users in KUMA must have unrestricted access to all events. You want to allow these users to view events from spaces that are not specified in the default set.

Action: The administrator goes to the **Access to spaces** section and selects the 'All spaces' set, which gives access to all spaces without restrictions, and grants access to this set to the selected users.

Result: Users that have been explicitly granted access to the 'All spaces' set now have unrestricted access to events in spaces. Their access to events depends only on the right to view the list of events in accordance with their assigned role. When you add new spaces or tenants, these users will have access to the events located in these new spaces and tenants, provided they have the right to view the list of events for the corresponding tenant. Users that have not been explicitly granted access to the 'All spaces' set will have restricted access to events in accordance with the default set of spaces.

Permitting some users to view events from a finite set of spaces

Goal: KUMA has a default set in which only a finite number of spaces is explicitly specified. Some users need to see a different space set, but not all available spaces.

Action: The administrator creates a space set that includes the relevant spaces and grants access to this set to the selected users.

Result: User access to events is restricted in accordance with the available space set. Users that have not been explicitly granted access to the set will have restricted access to events in accordance with the default set of spaces.

Supplementing an explicitly specified space set for a user

Goal: Users u1, u2, u3, u4 have been explicitly granted access to space set 'set1', which includes spaces to which Windows and Linux events go. Users u1 and u2, in addition to Windows and Linux events, need to view Cisco and VMware events that go to the respective spaces.

Action: The administrator creates a set of spaces, 'set2', which includes the spaces of Cisco and VMware events. The administrator assigns set2 to u1 and u2 in addition to set1.

Result: Users u1 and u2 now have access to events from the spaces of all of the sets available to them, that is, events from the set1 and set2: Windows, Linux, Cisco, VMware. Access of users u3 and u4 to events remains unchanged.

Editing a space set

Goal: Some users have access to a space set (access is granted explicitly or the set is the default set). For all of these users, you need to add access to a certain space that is not in the set, or revoke access to a space that is in the set.

Action: The administrator edits the existing set of spaces by adding or removing the relevant spaces.

Result: All users that have access to the set can now view events in accordance with the updated space set.

Deleting a space set

Goal: The space set is no longer relevant, and it needs to be deleted from KUMA.

Action: The administrator deletes an existing space set. The 'All spaces' set cannot be deleted. The default space set cannot be deleted.

Result: The deleted space set is gone from KUMA. All users that have been explicitly granted access to this set of spaces now have access to events in accordance with the space sets that remain available to them. If a user does not have any space sets left to which access has been explicitly granted, such a user's access to events is controlled by the default set.

Working with alerts

In KUMA, an *alert* is created when a sequence of events is received that triggers a correlation rule. Correlation rules are created by KUMA analysts to check incoming events for possible security threats, so when a correlation rule is triggered, a warning about possible malicious activity is displayed. Security officers responsible for data protection investigate these alerts and respond if necessary.

KUMA automatically assigns a severity to each alert. This parameter shows how important or numerous are the processes that triggered the correlation rule. Alerts with higher severity should be dealt with first. The severity value is automatically updated when new correlation events are received, but a security officer can also set it manually. In this case, the alert severity is no longer automatically updated.

Related events are linked to the alerts, which allows enriching alerts with data from these events. KUMA also offers drill down functionality for alert investigation.

You can use alerts to create incidents.

You can view and process alerts registered by the solution in the **Alerts** section. Alerts can be filtered. When you click the alert name, a window with its details opens.

Alert life cycle

Alert life cycle:

1. KUMA creates an alert when a correlation rule is triggered. The alert is named after the correlation rule that generated it. Alert is assigned the **New** status.

   Alerts with the **New** status continue to be updated with data when correlation rules are triggered. If the alert status changes, the alert is no longer updated with new events, and if the correlation rule is triggered again, a new alert is created.

2. A security officer assigns the alert to an operator for investigation. The alert status changes to **assigned**.

3. The operator performs one of the following actions:

   - Close the alert as false a positive (alert status changes to **closed**).

   - Respond to the threat and close the alert (alert status changes to **closed**).

   - Creates an incident based on the alert (the alert status changes to **In incident**).

Filling alerts with events

By default, the number of events associated with an alert cannot exceed 10,000. When the number of events associated with the alert reaches 10,000, a new alert is created with the same name, but with a new ID. You can view the alert ID in the alert details. If necessary, you can change this value in the properties of the segmentation rule in the **Correlation events limit** field. For this to work, the segmentation rule must be enabled and linked to the alert correlation rules of the tenant.

Alert segmentation

Using the segmentation rules, the stream of correlation events of the same type can be divided to create more than one alert.

Severity

Severity reflects the relative importance of security-sensitive activity detected by a KUMA correlator. It suggests the order in which alerts should be processed, and indicates whether senior security officers should be involved.

The correlator automatically assigns a severity value to correlation events and alerts based on correlation rule settings. The severity of an alert also depends on the assets related to the processed events because correlation rules take into account the severity of a related asset's category. If an alert or correlation event does not have any linked assets with a severity value, or if it does not have any linked assets at all, the alert or correlation event inherits the severity of the correlation rule that generated it. The severity of an alert or correlation event is always equal to or greater than the severity of the correlation rule that generated it.

If the event is linked to assets, the system uses the highest-severity asset category to calculate the severity of the correlation event or alert.

Example of formula for calculating the severity:

- If no assets with a severity level are linked to a correlation event or alert, or no assets are linked at all:
  - **Correlation event severity** = **Correlation rule severity**.
  - **Alert severity** = **Correlation rule severity**.
- If multiple assets are linked to an event or alert, then the highest severity among the categories of assets linked to the event or asset is taken as the **highest asset category severity**. If this value is greater than the severity of the correlation rule:
  - **Correlation event severity** = (**Correlation rule severity** + **Max asset category severity** + 1) / 2.
  - **Alert severity** = (**Correlation rule severity** + **Max asset category severity** + 1) / 2.

The severity of the correlation event can never be lower than the severity of the correlation rule. The correlator and collector must belong to the same tenant as the assets. Severities of the assets from other tenants are not taken into account.

Alert severity can be changed manually. A severity that has been manually modified is no longer automatically updated by correlation rules.

Possible severity values:

- 1 – Low
- 2 – Medium
- 3 – High
- 4 – Critical

Configuring alerts table

The main part of the **Alerts** section shows a table containing information about registered alerts.

The following columns are displayed in the alerts table:

- Severity ( )—shows the importance of a possible security threat: Critical , High , Medium , or Low .
- **Name**—alert name.
- **Status**—current status of an alert:
  - **New**—a new alert that hasn't been processed yet.
  - **Assigned**—the alert has been processed and assigned to a security officer for investigation or response.
  - **Closed**—the alert was closed. Either it was a false alert, or the security threat was eliminated.
  - **Escalated**—an incident was generated based on this alert.
- **Assigned to**—the name of the security officer the alert was assigned to for investigation or response.
- **Incident**—name of the incident to which this alert is linked.

- **Additional information** is the value of the field selected for display in the **Alert information** section when configuring alert filling. When you select some fields (for example, **SourceAddress**, **DestinationAddress**, **SourceUserName**, **DestinationUserName**), their associated fields are additionally displayed (**SourceAssetName**, **DestinationAssetName**, **SourceAccountName**, **DestinationAccountName**). The values of these fields are combined displayed in the **Additional information** column, separated by commas, in the following order: first the selected field, then the additional field.

  For the selected field, the earliest recorded and non-empty value of the event field associated with the alert is displayed.

  By default, this column is not displayed in the table. To add it, click the gear icon ( ) and select the check box next to the column title. .

- **First seen**—the date and time when the first correlation event of the event sequence was created, triggering creation of the alert.

- **Last seen**—the date and time when the last correlation event of the event sequence was created, triggering creation of the alert.

- **Categories**—categories of alert-related assets with the highest severity. No more than three categories are displayed.

- **Tenant**—the name of the tenant that owns the alert.

- **CII**—an indication whether the related to the alert assets are the CII objects. The column is hidden from the users who do not have access to CII objects.

You can view the alert filtering tools by clicking the column headers. When filtering alerts based on a specific parameter, the corresponding header of the alerts table is highlighted in yellow.

You can click the gear icon ( ), to customize the columns displayed in the alerts table.

In the **Search** field, you can use regular expressions to find alerts by their linked assets, users, tenants, or correlation rules. Parameters that can be used for a search:

- Assets: name, FQDN, IP address.

- Active Directory accounts: attributes displayName, SAMAccountName, and UserPrincipalName.

- Correlation rules: name.

- KUMA users who were assigned alerts: name, login, email address.

- Tenants: name.

Filtering alerts

In KUMA, you can perform alert selection by using the filtering and sorting tools in the **Alerts** section.

The filter settings can be saved. Existing filters can be deleted.

Saving and selecting an alert filter

In KUMA, you can save changes to the alert table settings as filters. Filters are saved on the KUMA Core server and are available to all KUMA users of the tenant for which they were created.

To save the current filter settings:

1. In the **Alerts** section of KUMA open the **Filters** drop-down list.
2. Select **Save current filter**.

   A field will appear for entering the name of the new filter and selecting the tenant that will own it.
3. Enter a name for the filter. The name must be unique for alert filters, incident filters, and event filters.
4. In the **Tenant** drop-down list, select the tenant that will own the filter and click **Save**.

The filter is saved.

To select a previously saved filter:

1. In the **Alerts** section of KUMA open the **Filters** drop-down list.
2. Select the relevant filter.

   To select the default filter, put an asterisk to the left of the relevant filter name in the **Filters** drop-down list.

The filter is selected.

To reset the current filter settings,

Open the **Filters** drop-down list and select **Clear filters**.

Deleting an alert filter

To delete a previously saved filter:

1. In the **Alerts** section of KUMA open the **Filters** drop-down list.
2. Click next to the configuration that you want to delete.
3. Click **OK**.

The filter is deleted for all KUMA users.

Viewing alert details

To view details on an alert:

1. In the solution's web interface window, select the **Alerts** section.

   The alerts table is displayed.

2. Click the name of the alert whose details you want to view.

   This opens a window containing information about the alert.

The upper part of the alert details window contains a toolbar and shows the alert severity and the user name to which the alert is assigned. In this window, you can process the alert: change its severity, assign it to a user, and close and create an incident based on the alert.

Details on alert section

This section lets you view basic information about an alert. It contains the following data:

- **Correlation rule severity** is the severity of the correlation rule that triggered the creation of the alert.
- **Max asset category severity**—the highest severity of an asset category assigned to assets related to this alert. If multiple assets are related to the alert, the largest value is displayed.
- **Linked to incident**—if the alert is linked to an incident, the name and status of the alert are displayed. If the alert is not linked to an incident, the field is blank.
- **First seen**—the date and time when the first correlation event of the event sequence was created, triggering creation of the alert.
- **Last seen**—the date and time when the last correlation event of the event sequence was created, triggering creation of the alert.
- **Alert ID**—the unique identifier of an alert in KUMA.
- **Tenant**—the name of the tenant that owns the alert.
- **Correlation rule**—the name of the correlation rule that triggered the creation of the alert. The rule name is represented as a link that can be used to open the settings of this correlation rule.

This section can additionally display the field of the correlation event and its value selected from the Display in Alert information drop-down list when **configuring alert filling**. For some of the fields, when they are selected, their associated fields are additionally displayed. For example, for the **SourceAddress** field, the additionally displayed field is **SourceAssetName**, for **DestinationAddress** it is **DestinationAssetName**, for **DeviceAddress** it is **DeviceAssetName**, for **SourceHostName it is SourceAssetName**, for **DestinationHostName** it is **DestinationAssetName**, for **DeviceHostName** it is **DeviceAssetName**. When you select the **SourceUserName** field, the **SourceAccountName** field is additionally displayed, and when you select **DestinationUserName**, **DestinationAccountName** is displayed. This works only in one direction, that is, for example, selecting the **DestinationAccountName** field does not display the **DestinationUserName** field.

For the selected field, the earliest recorded and non-empty value of the event field associated with the alert is displayed.

Related events section

This section contains a table of events related to the alert. If you click the arrow (›) icon near a correlation rule, the base events from this correlation rule will be displayed. Events can be sorted by severity and time.

Selecting an event in the table opens the details area containing information about the selected event. The details area also displays the **Detailed view** button, which opens a window containing information about the correlation event.

The **Find in events** links below correlation events and the **Find in events** button to the right of the section heading are used to go to alert investigation.

You can use the **Download events** button to download information about related events into a CSV file (in UTF-8 encoding). The file contains columns that are populated in at least one related event.

Some CSV file editors interpret the separator value (for example, \n) in the CSV file exported from KUMA as a line break, not as a separator. This may disrupt the line division of the file. If you encounter a similar issue, you may need to additionally edit the CSV file received from KUMA.

In the events table, in the event details area, in the alert window, and in the widgets, the names of assets, accounts, and services are displayed instead of the IDs as the values of the SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID, and ServiceID fields. When exporting events to a file, the IDs are saved, but columns with names are added to the file. The IDs are also displayed when you point the mouse over the names of assets, accounts, or services.

Searching for fields with IDs is only possible using IDs.

Related endpoints section

This section contains a table of assets related to the alert. Asset information comes from events that are related to the alert. You can search for assets by using the **Search for IP addresses or FQDN** field. Assets can be sorted using the **Count** and **Endpoint** columns.

This section also displays the assets related to the alert. Clicking the name of the asset opens the **Asset details** window. In that window, in the **Related alerts** section, in the **Find related alerts** drop-down list, you can select the period for which you want to find related alerts: last day, week, two weeks (default value), month, or year. After you select the period, the number of related alerts found is displayed. To view the full list, click the **Find in Alerts** button, to open the **Alerts** page with a filtered list of found related alerts.

You can use the **Download assets** button to download information about related assets into a CSV file (in UTF-8 encoding). The following columns are available in the file: **Count**, **Name**, **IP address**, **FQDN**, **Categories**.

Related users section

This section contains a table of users related to the alert. User information comes from events that are related to the alert. You can search for users using the **Search for users** field. Users can be sorted by the **Count**, **User**, **User principal name** and **Email** columns.

You can use the **Download users** button to download information about related users into a CSV file (in UTF-8 encoding). The following columns are available in the file: **Count**, **User**, **User principal name**, **Email**, **Domain**, **Tenant**.

Change log section

This section contains entries about changes made to the alert by users. Changes are automatically logged, but it is also possible to add comments manually. Comments can be sorted by using the **Time** column.

If necessary, you can enter a comment for the alert in the **Comment** field and click **Add** to save it.

Changing alert name

To change the alert name:

1. In the KUMA web interface window, select the **Alerts** section.

   The alerts table is displayed.

2. Click the name of the alert whose details you want to view.

   This opens a window containing information about the alert.

3. In the upper part of the window, click ✎ and in the field that opens, enter the new name of the alert. To confirm the name, press **ENTER** or click outside the entry field.

Alert name is changed.

Configuring alert filling

To configure alert filling:

1. In the KUMA web interface, go to the **Settings** → **Other** → **Alerts** section.

2. In the **Alerts** window, go to the **Alerts filling** tab and manage the following settings:

   a. In the **Status** drop-down list, select the status that an alert must have to be filled with events. The default setting is **New**. You can select multiple values. The **New** value cannot be removed from the selection. Available values:

      - **New** means the created correlation events continue to be linked to the alert only if the alert status is **New**.

      - **In incident** means the created correlation events continue to be linked to the alert only if the alert status is **In incident**. If the status of the alert changes to **In incident**, it can revert to the **New** status if the alert is unlinked from the incident. In that case, the filling of the alert with events stops.

        Example: the alert has the **In incident** status. While in the **In incident** status, no new events were received. If you unlink the alert from the incident, the alert will be filled with events. If, while the alert was linked to the incident, more events were received and a new alert was created, the last created alert is filled with events.

      - **Assigned** means the created correlation events continue to be linked to the alert only if the alert status is **Assigned**.

   b. In the **Alert was created no later than (hours)** field, specify the time during which the alert will be filled with events. The value must be an integer. The time is counted from the moment the alert is created. Default value: 336 hours (2 weeks). The minimum value is 1 hour.

      If some values are specified for the **Status**, **Alert was created time (hours)** and **Maximum number of events** settings, the filling of the alert is stopped when the first of the following conditions is satisfied:

      - The alert status has changed and no longer matches the selected values.

      - The specified filling time has run out.

      - The number of events in the alert has reached the value specified in the **Maximum number of events** field.

      If, after the alert has stopped filling, it regains a status in which filling is allowed, no new events are added to it. For example, if filling is configured only for the **New** status, filling stops after the alert transitions to the **In incident** status. If the alert then regains the **New** status, no new events are added to it.

   c. In the **Event storage** drop-down list, select the storage where the alert events are stored. Only one storage can be specified. The list shows storage resources, instead of running services. For alerts to be filled with events, the storage service must be running.

      Alerts created before specifying the storage in the filling settings do not contain any events. After the **Event storage** setting is specified or changed, existing alerts are not filled with events from the specified storage. In that case, new alerts are created with events from the specified storage. After selecting an event storage, this setting can take up to two minutes to be applied to alerts. Alerts created before this parameter is applied may not contain events from the specified storage.

d. In the **Display in Alert details** drop-down list, select the field of the correlation event to be displayed in the alert card and in the **Additional info** column in the **Alerts** section. You can select one of the following values:

- **DestinationAddress** is the IPv4 or IPv6 address of the destination (asset) involved in the event.
- **SourceAddress** is the IPv4 or IPv6 address of the device that was the source of the event. If the user logged in using a proxy server, the address of the proxy server is specified.
- **DeviceAddress** is the IPv4 or IPv6 address of the device from which the event was received.
- **DestinationAssetName** is the name of the asset at the destination.
- **SourceAssetName** is the name of the asset at the event source.
- **DeviceAssetName** is the name of the asset on the device from which the event was received.
- **DestinationHostName** is the domain name of the destination.
- **SourceHostName** is the domain name of the event source.
- **DeviceHostName** is the name of the device from which the event was received. FQDN of the device, if available.
- **DestinationUserName** is the user name of the destination.
- **SourceUserName** is the user name of the source.
- **DestinationAccountName** is the name of the account of the destination.
- **SourceAccountName** is the name of the account of the event source.
- **Message** is the brief description of the event.
- **DeviceCustomString1**, **DeviceCustomString2**, **DeviceCustomString3**, **DeviceCustomString4**, **DeviceCustomString5**, **DeviceCustomString6** are fields for mapping the string value.

You can select only one field. For some fields, an additional associated field is automatically displayed. If you select a field that refers to an address or host name, the associated **AssetName** field is additionally displayed. If you selected a field associated with a user name, the **AccountName** field is additionally displayed. In these cases, the field values are combined with a comma: the selected field comes first and is followed by the additional field.

The modified setting applies only to new alerts.

e. In the **Maximum number of events** field, specify the maximum number of events that can be added to one alert. After the specified amount is reached, filling of the alert stops.

The value must be an integer. The default value is `10000`. The minimum value is `1`. No maximum value is set.

When you save segmentation rules, the value of the number of events is checked. If the number of events specified in the rule is greater than the value of the Maximum number of events setting, the saving process finishes with an error. For segmentation rules created before the value of the setting was decreased, the change is not applied. Such rules continue to work, but the number of events added to an alert never exceeds the value of the **Maximum number of events** setting.

Alert filling is configured.

Processing alerts

You can change the alert severity, assign an alert to a user, close the alert, or create an incident based on the alert.

To process an alert:

1. Select required alerts using one of the methods below:

   - In the **Alerts** section of the KUMA web interface, click the alert whose information you want to view.

     The Alert window opens and provides an alert processing toolbar at the top.

   - In the **Alerts** section of the KUMA web interface, select the check box next to the required alert. It is possible to select more than one alert.

     > Alerts with the **closed** status cannot be selected for processing.

     A toolbar will appear at the bottom of the window.

2. If you want to change the severity of an alert, select the required value in the **Severity** drop-down list:

   - **Low**
   - **Medium**
   - **High**
   - **Critical**

   The severity of the alert changes to the selected value.

3. If you want to assign an alert to a user, select the relevant user from the **Assign to** drop-down list.

   You can assign the alert to yourself by selecting **Me**.

   The status of the alert will change to **Assigned** and the name of the selected user will be displayed in the **Assign to** drop-down list.

4. In the **Related users** section, select a user and configure Active Directory response settings.

   a. After the related user is selected, in the **Account details** window that opens, click **Response via Active Directory**.

   b. In the **AD command** drop-down list, select one of the following values:

      - **Add account to group**

        Specify the Active Directory group to which you want to add the user account. In the **Distinguished name** field, enter the full path to the group, for example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com.

        Only one group can be specified.

      - **Remove account from group**

Specify the Active Directory group from which you want to remove the user account. In the **Distinguished name** field, enter the full path to the group, for example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com.

Only one group can be specified.

- **Reset account password**
- **Block account**

c. Click **Apply**.

5. If required, create an incident based on the alert:

a. Click **Create incident**.

The window for creating an incident will open. The alert name is used as the incident name.

b. Update the desired incident parameters and click the **Save** button.

The incident is created, and the alert status is changed to **Escalated**. An alert can be unlinked from an incident by selecting it and clicking **Unlink**.

6. If you want to close the alert:

a. Click **Close alert**.

A confirmation window opens.

b. Select the reason for closing the alert:

- **Responded**. This means the appropriate measures were taken to eliminate the security threat.
- **Incorrect data**. This means the alert was a false positive and the received events do not indicate a security threat.
- **Incorrect correlation rule**. This means the alert was a false positive and the received events do not indicate a security threat. The correlation rule may need to be updated.

c. Click **OK**.

The status of the alert is changed to **Closed**. Alerts with this status are no longer updated with new correlation events and aren't displayed in the alerts table unless the **Closed** check box is selected in the **Status** drop-down list in the alerts table. You cannot change the status of a closed alert or assign it to another user.

Alert investigation

Alert investigation is used when you need to find more information about the threat that triggered the alert: is the threat real, what is its origin, what elements of the network environment are affected by it, how should the threat be dealt with. Studying the events related to the correlation events that triggered an alert can help you determine the course of action.

For convenience of investigating alerts, make sure that time is synchronized on all devices involved in the event life cycle (event sources, KUMA servers, client hosts) with the help of Network Time Protocol (NTP) servers.

The alert investigation mode is enabled in KUMA when you click the **Find in events** link in the alert window or the correlation event window. When the alert investigation mode is enabled, the events table is shown with filters automatically set to match the events from the alert or correlation event. The filters also match the time period of the alert duration or the time when the correlation event was registered. You can change these filters to find other events and learn more about the processes related to the threat.

An additional drop-down list becomes available in alert investigation mode:

- **All events**—view all events.
- **Related to alert** (selected by default)—view only events related to the alert.

  When filtering events related to an alert, there are limitations on the complexity of SQL search queries.

You can manually assign an event of any type except the correlation event to an alert. Only events that are not related to the alert can be linked to it.

You can create and save event filters in alert investigation mode. When using this filter in normal mode, all events that match the filter criteria are selected regardless of whether or not they are related to the alert that was selected for alert investigation.

To link an event to an alert:

1. In the **Alerts** section of the KUMA web interface, click the alert that you want to link to the event.

   The Alert window opens.

2. In the **Related events** section, click the **Find in events** button.

   The events table is opened and displayed with active date and time filters matching the date and time of events linked to the alert. The columns show the settings used by the correlation rule to generate the alert. The **Link to alert** column is also added to the events table showing the events linked to the alert.

3. In the drop-down list select **All events**.

4. If necessary, modify the filters to find the event that you need to link to the alert.

5. Select the relevant event and click the **Link to alert** button in the lower part of the event details area.

   The event will be linked to the alert. You can unlink this event from the alert by clicking in the **Unlink from alert** detailed view.

When an event is linked to or unlinked from an alert, a corresponding entry is added to the **Change log** section in the Alert window. You can click the link in this entry to open the details area and unlink or link the event to the alert by clicking the corresponding button.

Retention of alerts and incidents

The alert and incident retention conditions are determined by the following criteria:

- Retention period. By default, KUMA retains alerts and incidents for 365 days, but you can set a different period by changing the **Alert retention period, days** setting.

- Deletion conditions. After the expiration of the specified retention period, if certain conditions are satisfied, alerts and incidents may be retained further.

There are no limitations on the size of a stored alert.

Setting the retention period for alerts and incidents

To change the retention period for alerts and incidents in the KUMA web interface:

1. In the KUMA web interface, go to the **Settings** → **Other** → **General** section.

2. In the **General** window, under **Core properties**, specify the **Alert retention period, days**.

   The retention period for alerts and incidents will be changed.

Alert and incident deletion conditions

KUMA applies the following alert and incident deletion conditions:

- If an alert is older than the retention period, its events are deleted regardless of the alert status.

- If an alert is older than the retention period, has the **Closed** status, and is not linked to an incident, the alert is deleted.

- If an alert is older than the retention period (regardless of the alert status) and is linked to an incident whose retention period has not yet expired, the alert events are deleted, the alert without events is available for display and remains linked to the incident without the events.

- If the incident is older than the retention period, the status of the incident is **Closed**, and it has no linked alerts, the incident is deleted.
- If an incident is older than the retention period, the status of the incident is **Closed**, and only alerts older than the retention period are linked to it (the status of alerts linked to a closed incident is always **Closed, incident closed**), the incident is deleted together with all its alerts and events.
- If an incident is older than the retention period (regardless of the status of the incident), and it has linked alerts that have not yet expired, nothing is deleted.
- If an incident is older than the retention period, has a status other than **Closed**, and alerts older than the retention period are linked to the incident, the incident is not deleted, alerts are not deleted, but events of the alerts are deleted.
- Empty alerts (alerts without events whose retention period has expired) are deleted together with incidents when the incident satisfies deletion conditions in accordance with the retention period are satisfied (the incident has the **Closed** status and its retention period has expired).
- If an incident is older than the retention period, the status of the incident is **Closed**, and it has linked alerts that are older than the retention period and some alerts that fall within the retention period, such an incident is not deleted. Alerts whose retention period has not expired are not deleted. Events of alerts whose retention period has expired are deleted and the alerts themselves remain empty and linked to the incident.

Alert notifications

Standard KUMA notifications are sent by email when alerts are generated and assigned. You can configure delivery of alert generation notifications based on a custom email template.

Creating a notification rule

To configure delivery of alert generation notifications based on a custom template:

1. In the KUMA web interface, open the **Settings** → **Other** → **Alerts** → **Notification rules** section.
2. Select the tenant for which you want to create a notification rule:
   - If the tenant already has notification rules, select it in the table.
   - If the tenant does not have notification rules, click **Add settings for a new tenant**.
3. This opens the **Notification rule settings** window; in that window, manage the following settings:
   - If you want the rule to be applied after saving the settings, enable the **State** toggle switch.
   - In the **Tenant** drop-down list, select a tenant.

4. Under **Notification rules**, click **Add** and specify the notification rule settings:

   - **Name** (required)—specify the notification rule name in this field.

   - **Recipient emails** (required)—in this group of settings, you can use the **Email** button to add the email addresses to which you want to send notifications about alert generation. Addresses are added one at a time.

     Email addresses must contain only ASCII characters.

   - **Correlation rules** (required)—in this settings block, you must select one or more correlation rules that, when triggered, will cause notification sending.

     The window displays a tree structure representing the correlation rules from the shared tenant and the user-selected tenant. To select a rule, select the check box next to it. You can select the check box next to a folder to select all correlation rules in that folder and its subfolders.

   - **Template** (required)—in this settings block, you must select a notification template that will be used to create the notifications. To select a template, click the icon, select the required template in the opened window, and click **Save**.

     You can create a template by clicking the plus icon or edit the selected template by clicking the pencil icon.

   - **Disabled**—by selecting this check box, you can disable the notification rule.

5. Click **Save**.

The notification rule is created. When an alert is created based on the selected correlation rules, notifications created based on custom email templates will be sent to the specified email addresses. Standard KUMA notifications about the same event will not be sent to the specified addresses.

Duplicating the settings of a notification rule

To duplicate alert notification settings:

1. Open notification rules:

   a. In the KUMA web interface, go to the **Settings** → **Other** → **Alerts** → **Notification rules** section.

   b. In the table of tenants, select the tenant whose notification rule settings you want to duplicate. Selecting a tenant opens the **Notification rule settings** window.

2. Copy the settings of the original rule:

   a. In the **Notification rule settings** window, in the **Notification rules** section, open the rule that you need.

      This opens the **Edit notification rule** window.

   b. In the **Edit notification rule** window, click the **Copy** button.

      The **Paste** button becomes available only after you click the **Copy** button.

      You can copy within a tenant or between tenants.

   c. Click the (×) button or click **Cancel** to close the **Edit notification rule** window.

3. Preparing for pasting:

   - If you want to duplicate settings within the same tenant, proceed to the next step.
   - If you want to use the copied settings in another tenant:
     1. Close the **Notification rule settings** window for the current tenant.
     2. Navigate to your target tenant. Selecting a tenant opens the **Notification rule settings** window.

4. Pasting settings:

   a. In the **Notification rule settings** window, click **Add**.

   b. This opens the **Edit notification rule** window; in that window, click the **Paste** button.

5. Checking and editing fields. After pasting, the following settings are duplicated, and the corresponding fields are pre-filled:

   - The **State** toggle switch is set to the same position as in the original rule.
   - In the **Name** field, enter a new name for the rule. You cannot save the copy with the same name as the original rule.
   - The list of **Recipient addresses** is duplicated. You can change the port if necessary.
   - **Tenants and correlation rules**.

     The behavior of the tree of correlation rules depends on whether the rule belongs to the tenant:

     - If you copy and paste settings within a tenant, after pasting, the rules from the source notification rule automatically become selected.
     - If you copy and paste between tenants, but the correlation rule is in the Shared tenant, after pasting, the correlation rules from the original notification rule are automatically selected in the tree of correlation rules.
     - If you copy and paste between tenants, and the correlation rule is not in the Shared tenant, an access error is returned after pasting. In this case, you need to manually specify the tenant and the correlation rules.
   - The same **Template** is set as in the source rule.

   If necessary, edit the pasted settings.

6. Click **Save**.

The settings of the notification rule are duplicated.

Disabling a notification rule

To disable notification rules for a tenant:

1. In the KUMA web interface, open the **Settings** → **Other** → **Alerts** → **Notification rules** section and select the tenant whose notification rules you want to disable.

2. Select the **Disabled** check box.

3. Click **Save**.

The notification rules of the selected tenant are disabled.

For disabled notification rules, the correctness of the specified parameters is not checked; at the same time, notifications cannot be enabled for a tenant if incorrect rules exist. If you create or edit individual notification rules with tenant notification rules disabled, before enabling tenant notification rules, it is recommended to: 1) disable all individual notification rules, 2) enable tenant notification rules, 3) enable individual notification rules one by one.

Working with incidents

If the nature of the data received by KUMA or the generated correlation events and alerts indicate a possible attack or vulnerability, the symptoms of such an occurrence can be combined into an *incident*. This allows security officers to analyze threat manifestations in a comprehensive manner and facilitates response.

You can assign a category, type, and severity to an incident, and assign incidents to data protection officers for processing.

You can create, view and process incidents in the **Incidents** section. You can also filter incidents if needed. Clicking the name of an incident opens a window containing information about the incident.

Incidents can be exported to NCIRCC.

The retention period for incidents is one year, but this setting can be changed.

Viewing incidents

The main part of the **Incidents** section shows a table containing information about registered incidents. If required, you can change the set of columns and the order in which they are displayed in the table.

How to customize the incidents table

1. Click the gear (⚙) icon in the upper-right corner of the incidents table.

   The table customization window opens.

2. Select the check boxes opposite the settings that you want to view in the table.

When you select a check box, the events table is updated and a new column is added. When a check box is cleared, the column disappears.

You can search for table parameters using the **Search** field.

By pressing the **Default** button, the following columns are selected for display:

- **Name**.
- **Threat duration**.
- **Assigned**.
- **Created**.
- **Tenant**.
- **Status**.
- **Hits count**.
- **Severity**.
- **Affected asset categories**.

3. Change the display order of the columns as needed by dragging the column headings.
4. If you want to sort the incidents by a specific column, click its title and select one of the available options in the drop-down list: **Ascending** or **Descending**.
5. To filter incidents by a specific parameter, click on the column header and select the required filters from the drop-down list. The set of filters available in the drop-down list depends on the selected column.
6. To remove filters, click the relevant column heading and select **Clear filter**.

Available columns of the incidents table:

- **Name**—the name of the incident. If necessary, you can copy the link from the incident name without drilling down to the incident information.

  Names of incidents received from NCIRCC have the ALRT* prefix.

- **Threat duration**—the time span during which the incident occurred (the time between the first and the last event related to the incident).
- **Assigned to**—the name of the security officer to whom the incident was assigned for investigation or response.
- **Created**—the date and time when the incident was created. This column allows you to filter incidents by the time they were created.
  - The following preset periods are available: **Today**, **Yesterday**, **This week**, **Previous week**.
  - If necessary, you can set an arbitrary period by using the calendar that opens when you select **Before date**, **After date**, **In period**.
- **UUID**—Unique ID of the incident.

  By default, the UUID value is hidden.

- **Tenant**—the name of the tenant that owns the incident.
- **Status**—current status of the incident:
  - **Opened**—new incident that has not been processed yet.
  - **Assigned**—the incident has been processed and assigned to a security officer for investigation or response.
  - **Closed**—the incident is closed; the security threat has been resolved.
- **Alerts number**—the number of alerts included in the incident. Only the alerts of those tenants to which you have access are taken into account.
- **Severity** shows how important a possible security threat is: **Critical**, **High**, **Medium**, **Low**.
- **Affected asset categories**—categories of alert-related assets with the highest severity. No more than three categories are displayed.
- **Updated**—the date and time of the last change made in the incident.
- **First event** and **Last event**—dates and times of the first and last events in the incident.
- **Incident category** and **Incident type**—category and type of threat assigned to the incident.
- **Export to NCIRCC**—the status of incident data export to NCIRCC:
  - **Not exported**—the data was not forwarded to NCIRCC.
  - **Export failed**—an attempt to forward data to NCIRCC ended with an error, and the data was not transmitted.
  - **Exported**—data on the incident has been successfully transmitted to NCIRCC.
- **Branch**—data on the specific node where the incident was created. Incidents of your node are displayed by default. This column is displayed only when hierarchy mode is enabled.
- **CII**—an indication of whether the incident involves assets that are CII objects. The column is hidden from the users who do not have access to CII objects.

You can filter incidents by category of affected asset. You can select one or more categories.

When filtering incidents based on a specific parameter, the header of the corresponding column in the incidents table is highlighted in yellow.

In the **Search** field, you can enter a regular expression for searching incidents based on their related assets, users, tenants, and correlation rules. Parameters that can be used for a search:

- Assets: name, ID, FQDN, IP address, MAC address.
- Active Directory accounts: attributes displayName, SAMAccountName, and UserPrincipalName.
- Correlation rules: name.
- KUMA users who were assigned alerts: name, login, email address.

- Tenants: name.

  You can select one or more values from the list of tenants.

There is no searching by UUID.

Saving and selecting incident filter configuration

In KUMA, you can save changes to incident table settings as filters. Filter configurations are saved on the KUMA Core server and are available to all KUMA users of the tenant for which they were created.

To save the current filter configuration settings:

1. In the **Incidents** section of KUMA, open the **Select filter** drop-down list.

2. Select **Save current filter**.

   A window will open for entering the name of the new filter and selecting the tenant that will own the filter.

3. Enter a name for the filter configuration. The name must be unique for alert filters, incident filters, and event filters.

4. In the **Tenant** drop-down list, select the tenant that will own the filter and click **Save**.

The filter configuration is now saved.

To select a previously saved filter configuration:

1. In the **Incidents** section of KUMA, open the **Select filter** drop-down list.

2. Select the configuration you want.

The filter configuration is now active.

> You can select the default filter by putting an asterisk to the left of the required filter configuration name in the **Filters** drop-down list.

To reset the current filter settings,

open the **Filters** drop-down and select **Clear filter**.

Deleting incident filter configurations

To delete a previously saved filter configuration:

1. In the **Incidents** section of KUMA, open the **Filters** drop-down list.
2. Click the button next to the configuration you want to delete.
3. Click **OK**.

   The filter configuration is now deleted for all KUMA users.

Viewing incident details

To view information about an incident:

1. In the solution web interface window, select the **Incidents** section.
2. Select the incident whose information you want to view.

   This opens a window containing information about the incident.

Some incident parameters are editable. Incidents automatically created in KUMA based on a notification from NCIRCC have the ALRT* prefix.

In the upper part of the Incident details window, there is a toolbar and the name of the user to whom the incident is assigned. The window sections are displayed as tabs. You can click a tab to move to the relevant section. In this window, you can process the incident: assign it to a user, combine it with another incident, or close it.

The **Description** section contains the following data:

- **Created**—the date and time when the incident was created.
- **Name**—the name of the incident.

  You can change the name of an incident by entering a new name in the field and clicking **Save** The name must contain 1 to 128 Unicode characters.
- **Tenant**—the name of the tenant that owns the incident.

  The tenant can be changed by selecting the required tenant from the drop-down list and clicking **Save**
- **Status**—current status of the incident:
  - **Opened**—new incident that has not been processed yet.
  - **Assigned**—the incident has been processed and assigned to a security officer for investigation or response.
  - **Closed**—the incident is closed; the security threat has been resolved.

- **Severity**—the severity of the threat posed by the incident. Possible values:
  - **Critical**
  - **High**
  - **Medium**
  - **Low**

  Severity can be changed by selecting the required value from the drop-down list and clicking **Save**.
- **Affected asset categories**—the assigned categories of assets associated with the incident.
- **First event time** and **Last event time**—dates and times of the first and last events in the incident.
- **Type** and **Category**—type and category of the threat assigned to the incident. You can change these values by selecting the relevant value from the drop-down list and clicking **Save**.
- **Export to NCIRCC**—information on whether or not this incident was exported to NCIRCC.
- **Description**—description of the incident.

  To change the description, edit the text in the field and click **Save**. The description can contain no more than 256 Unicode characters.
- **Related tenants**—tenants associated with incident-related alerts, assets, and users.
- **Available tenants**—tenants whose alerts can be linked to the incident automatically.

  The list of available tenants can be changed by checking the boxes next to the required tenants in the drop-down list and clicking **Save**.

The **Related alerts** section contains a table of alerts related to the incident. When you click on the alert name, a window opens with detailed information about this alert.

The **Related endpoints** and **Related users** sections contain tables with data on assets and users related to the incident. This information comes from alerts that are related to the incident.

You can add data to the tables in the **Related alerts**, **Related endpoints** and **Related users** sections by clicking the **Link** button in the appropriate section and selecting the object to be linked to the incident in the opened window. If required, you can unlink objects from the incident. To do this, select the objects as required, click **Unlink** in the section to which they belong, and save the changes. If objects were automatically added to the incident, they cannot be unlinked until the alert mentioning those objects is unlinked. The set of the fields in the tables can be changed by clicking the gear (⚙) button in the relevant section. You can search the data in the tables of these sections using the **Search** fields.

The **Change log** section contains a record of the changes you and your users made to the incident. Changes are automatically logged, but it is also possible to add comments manually.

In the **NCIRCC integration** section, you can monitor the incident status in NCIRCC. In this section, you can also export incident data to NCIRCC, send files to NCIRCC, and exchange messages with NCIRCC experts.

If incident settings have been modified on the NCIRCC side, a corresponding notification is displayed in the incident window in KUMA. In this case, for the settings whose values were modified, the window displays the values from KUMA and the values from NCIRCC.

Incident creation

To create an incident:

1. Open the KUMA web interface and select the **Incidents** section.

2. Click **Create incident**.

   The window for creating an incident will open.

3. Fill in the mandatory parameters of the incident:

   - In the **Name** field enter the name of the incident. The name must contain 1 to 128 Unicode characters.

   - In the **Tenant** drop-down list, select the tenant that owns the created incident.

4. If necessary, provide other parameters for the incident:

   - In the **Severity** drop-down list, select the severity of the incident. Available options: **Low**, **Medium**, **High**, **Critical**.

   - In the **First event time** and **Last event time** fields, specify the time range in which events related to the incident were received.

   - In the **Category** and **Type** drop-down lists, select the category and type of the incident. The available incident types depend on the selected category.

   - Add the incident **Description**. The description can contain no more than 256 Unicode characters.

   - In the **Available tenants** drop-down list, select the tenants whose alerts can be linked to the incident automatically.

   - In the **Related alerts** section, add alerts related to the incident.

     Linking alerts to incidents

     To link an alert to an incident:

     1. In the **Related alerts** section of the incident window click **Link**.

        A window with a list of alerts not linked to incidents will open.

     2. Select the required alerts.

        PCRE regular expressions can be used to search alerts by user, asset, tenant, and correlation rule.

     3. Click **Link**.

     Alerts are now related to the incident and displayed in the **Related alerts** section.

To unlink alerts from an incident:

1. Select the relevant alerts in the **Related alerts** section and click **Unlink**.
2. Click **Save**.

   Alerts have been unlinked from the incident. Also, the alert can be unlinked from the incident in the alert window using the **Unlink** button.

- In the **Related endpoints** section, add assets related to the incident.

  Linking assets to incidents

  To link an asset to an incident:

  1. In the **Related endpoints** section of the incident window, click **Link**.

     A window containing a list of assets will open.
  2. Select the relevant assets.

     You can use the **Search** field to look for assets.
  3. Click **Link**.

  Assets are now linked to the incident and are displayed in the **Related endpoints** section.

  To unlink assets from an incident:

  1. Select the relevant assets in the **Related endpoints** section and click **Unlink**.
  2. Click **Save**.

  The assets are now unlinked from the incident.

- In the **Related users** section, add users related to the incident.

  Linking users to incidents

  To link a user to an incident:

  1. In the **Related users** section of the incident window, click **Link**.

     The user list window opens.
  2. Select the required users.

     You can use the **Search** field to look for users.
  3. Click **Link**.

  Users are now linked to the incident and appear in the **Related users** section.

To unlink users from the incident:

1. Select the required users in the **Related users** section and click the **Unlink** button.
2. Click **Save**.

   Users are unlinked from the incident.

- Add a **Comment** to the incident.

5. Click **Save**.

The incident has been created.

Incident processing

For convenience of processing incidents, make sure that time is synchronized by means of Network Time Protocol (NTP) servers across all devices involved in the event processing life cycle (event sources, KUMA servers, client hosts).

You can assign an incident to a user, aggregate it with other incidents, or close it.

To process an incident:

1. Select required incidents using one of the methods below:

   - In the **Incidents** section of the KUMA web interface, click the incident to be processed.

     The incident window will open, displaying a toolbar on the top.

   - In the **Incidents** section of the KUMA web console, select the check box next to the required incidents.

     A toolbar will appear at the bottom of the window.

2. In the **Assign to** drop-down list, select the user to whom you want to assign the incident.

   You can assign the incident to yourself by selecting **Me**.

   The status of the incident changes to **assigned** and the name of the selected user is displayed in the **Assign to** drop-down list.

3. In the **Related users** section, select a user and configure Active Directory response settings.

   a. After the related user is selected, in the **Account details** window that opens, click **Response via Active Directory**.

   b. In the **AD command** drop-down list, select one of the following values:

      - **Add account to group**

        Specify the Active Directory group to which you want to add the user account. In the **Distinguished name** field, enter the full path to the group, for example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com.

        Only one group can be specified.

- **Remove account from group**

  Specify the Active Directory group from which you want to remove the user account. In the **Distinguished name** field, enter the full path to the group, for example, CN=Team,OU=Groups,OU=ExchangeObjects,DC=example,DC=com.

  Only one group can be specified.

- **Reset account password**

- **Block account**

c. Click **Apply**.

4. If required, edit the incident parameters.

5. After investigating, close the incident:

   a. Click **Close**.

   A confirmation window opens.

   b. Select the reason for closing the incident:

   - **confirmed**. This means the incident was valid and appropriate measures were taken to eliminate the security threat.

   - **not confirmed**. This means the incident was a false positive and the received events do not indicate a security threat.

   c. Click **Close**.

   The **Closed** status will be assigned to the incident. Incidents with this status cannot be edited, and they are displayed in the incidents table only if you selected the **Closed** check box in the **Status** drop-down list when filtering the table. You cannot change the status of a closed incident or assign it to another user, but you can aggregate it with another incident.

6. If requited, aggregate the selected incidents with another incident:

   a. Click **Merge**. In the opened window, select the incident in which all data from the selected incidents should be placed.

   b. Confirm your selection by clicking **Merge**.

   The incidents will be aggregated.

The incident has been processed.

Changing incidents

To change the parameters of an incident:

1. In the **Incidents** section of the KUMA web interface, click on the incident you want to modify.

   The Incident window opens.

2. Make the necessary changes to the parameters. All incident parameters that can be set when creating it are available for editing.

3. Click **Save**.

The incident will be modified.

Automatic linking of alerts to incidents

In KUMA, you can configure automatic linking of generated alerts to existing incidents if alerts and incidents have related assets or users in common. If this setting is enabled, when creating an alert the solution searches for incidents falling into a specified time interval that includes assets or users from the alert. In addition, the solution checks whether the generated alert pertains to the tenants specified in the incidents' **Available tenants** parameter. If a matching incident is found, the solution links the generated alert to the incident it found.

To set up automatic linking of alerts to incidents:

1. In the KUMA web interface, open **Settings** → **Incidents** → **Automatic linking of alerts to incidents**.

2. Select the **Enable** check box in the **Link by assets** and/or **Link by accounts** groups of settings depending on the types of connections between incidents and alerts that you are looking for.

3. Define the **Incidents must not be older than** value for the parameters that you want to use when searching links. The generated alerts will be compared with incidents no older than the specified interval.

Automatic linking of alerts to incidents is configured.

To disable automatic linking of alerts to incidents,

In the KUMA web interface, under **Settings** → **Incidents** → **Automatic linking of alerts to incidents**, select the **Disabled** check box.

Categories and types of incidents

For your convenience, you can assign categories and types. If an incident has been assigned a NCIRCC category, it can be exported to NCIRCC.

Categories and types of incidents that can be exported to NCIRCC

The table below lists the categories and types of incidents that can be exported to NCIRCC:

Incident category	Incident type
Computer incident notification	Slowed operation of the resource due to a DDoS attack
	Malware infection
	Network traffic interception
	Compromised user account
	Unauthorized data modification
	Unauthorized disclosure of information
	Publication of illegal information on the resource
	Successful exploitation of a vulnerability
	Event is not related to a computer attack
	Use of a controlled resource for attacks
Notification about a computer attack	DDoS attack
	Unsuccessful authorization attempts
	Malware injection attempts
	Attempts to exploit a vulnerability
	Publication of fraudulent information
	Network scanning
	Social engineering
Notification about a detected vulnerability	Vulnerable resource

The categories of incidents can be viewed or changed under **Settings** → **Incidents** → **Incident types**, in which they are displayed as a table. By clicking on the column headers, you can change the table sorting options. The resource table contains the following columns:

- **Category**—a common characteristic of an incident or cyberattack. The table can be filtered by the values in this column.
- **Type**—the class of the incident or cyberattack.
- **NCIRCC category**—incident type according to NCIRCC nomenclature. Incidents that have been assigned custom types and categories cannot be exported to NCIRCC. The table can be filtered by the values in this column.
- **Vulnerability**—specifies whether the incident type indicates a vulnerability.
- **Created**—the date the incident type was created.
- **Updated**—the date the incident type was modified.

To add an incident type:

1. In the KUMA web interface, under **Settings** → **Incidents** → **Incident types**, click **Add**.

   The incident type creation window will open.

2. Fill in the **Type** and **Category** fields.
3. If the created incident type matches the NCIRCC nomenclature, select the **NCIRCC category** check box.

4. If the incident type indicates a vulnerability, check **Vulnerability**.

5. Click **Save**.

   The incident type has been created.

Interaction with NCIRCC

In KUMA, you can interact with the National Computer Incident Response & Coordination Center (hereinafter NCIRCC) in the following ways:

- Export incidents to NCIRCC.
- Supplement the exported incident with data when requested by NCIRCC.
- Send files to NCIRCC.
- Exchange messages with NCIRCC experts.
- View the changes made by NCIRCC to the parameters of exported incidents.
- Process incidents with the ALRT* prefix that are automatically created in KUMA based on a notification from NCIRCC.

Data in KUMA and NCIRCC is synchronized every 5-10 minutes.

Conditions for NCIRCC interaction

To interact with NCIRCC, the following conditions must be met:

- The solution license includes the GosSOPKA module.
- NCIRCC integration is configured.
- The **Can interact with NCIRCC** check box is selected in the settings of the users whose responsibilities include interaction with NCIRCC.

NCIRCC interaction workflow

In KUMA, the process of sending incidents to NCIRCC to be processed consists of the following stages:

1. **Creating an incident and checking it for compliance with NCIRCC requirements**

   You can create an incident or get it from a child KUMA node. Before sending data to the NCIRCC, make sure that the incident category meets NCIRCC requirements.

2. **Exporting the incident to NCIRCC**

If the incident is successfully exported to NCIRCC, its **Export to NCIRCC** setting is set to **Exported**. In the lower part of the incident window, a chat with NCIRCC experts becomes available.

At NCIRCC, the incident received from you is assigned a registration number and status. This information is displayed in the incident window in the **NCIRCC integration** section and in automatic chat messages.

If all the necessary data is provided to NCIRCC, the incident is assigned the **Under examination** status. The settings of the incident having this status can be edited, but the updated information cannot be sent from KUMA to NCIRCC. You can view the difference between the incident data in KUMA and in NCIRCC.

3. **Supplementing incident data**

   If NCIRCC experts do not have enough information to process an incident, they can assign it the **More information required** status. In KUMA, this status is displayed in the incident window in the **NCIRCC integration** section. Users are notified about the status change.

   If necessary, you can attach a file to the incident.

   When the data is supplemented, the incident is re-exported to NCIRCC with earlier information updated. The incidents in the child nodes cannot be modified from the parent KUMA node. It must be done by employees of the child KUMA nodes.

   If the incident is successfully supplemented with data, it is assigned the **Under examination** status.

4. **Completing incident processing**

   After the NCIRCC experts process the incident, the NCIRCC status is changed to **Decision made**. In KUMA, this status is displayed in the incident window in the **NCIRCC integration** section.

   Upon receiving this status, the incident is automatically closed in KUMA. Interaction with NCIRCC on this incident by means of KUMA becomes impossible.

Exporting data to RuCERT

To export an incident to NCIRCC:

1. In the **Incidents** section, open the incident you want to export.

2. Click the **Export to NCIRCC** button in the lower part of the window.

3. If you have not specified the category and type of incident, specify this information in the window that opens and click the **Export to NCIRCC** button.

   This opens the export settings.

   If you specified the category and type of the incident in the incident card, save the incident before exporting it to NCIRCC.

4. In the **Export to NCIRCC** window, open the **Basic** tab.

5. On the **Basic settings** tab, fill in the required fields:

   Company name, **Asset owner**, Incident category, Incident type, **Summary**, **TLP**, **Incident creation date**, **Status**, **Affected system name**, Affected system category, **Affected system function**, **Location**.

   Possible values of the TLP parameter

   - WHITE—disclosure is not restricted.

   - GREEN—disclosure is only for the community.

- AMBER—disclosure is only for organizations.
- RED—disclosure is only for a specific group of people.

Possible values for the Affected system function parameter

- Nuclear energy
- Banking and other financial market sectors
- Mining
- Federal/municipal government
- Healthcare
- Metallurgy
- Science
- Defense industry
- Education
- Aerospace industry
- Communication
- Mass media
- Fuel and power
- Transportation
- Chemical industry
- Other
- If you want to provide information about a personal data leak, select the **Information about PD leakage** check box and manage the settings on **Information about PD leakage** tab. This check box is cleared by default.

  The **Operator name**, **INN**, and **Operator address** fields are populated automatically with the values specified when setting up the NCIRCC integration. However, the field values can be edited when preparing the data export to NCIRCC.

  Personal data leak fields are available for the **Notification about a computer incident** category for the following notification types:

  - **Malware infection**
  - **Compromised user account**
  - **Unauthorized disclosure of information**

- **Successful exploitation of a vulnerability**
- **Event is not related to a computer attack**

- **Product info** (required)—this table becomes available if you selected **Notification about a detected vulnerability** as the incident category.

  You can use the **Add new element** button to add a string to the table. In the **Name** column, you must indicate the name of the application (for example, `MS Office`). Specify the application version in the **Version** column (for example, `2.4`).

- As the **Vulnerability ID**, if necessary, specify the ID of the detected vulnerability, for example, `CVE-2020-1231`.

  This field becomes available if you selected **Notification about a detected vulnerability** as the incident category.

- As the **Product category**, if necessary, specify the name and version of the affected product, for example, `Microsoft operating systems and their components`.

  This field becomes available if you selected **Notification about a detected vulnerability** as the incident category.

6. If required, define the settings on the **Advanced** tab of the **Export to NCIRCC** window.

   The available settings on the tab depend on the selected category and type of incident:

   - **Detection tool**—specify the name of the product that was used to register the incident. For example, `KUMA 1.5`.
   - **Assistance required**—select this check box if you need help from GosSOPKA employees.
   - **Incident end time**—specify the date and time when the critical information infrastructure (CII object) was restored to normal operation after a computer incident, computer attack was ended, or a vulnerability was fixed.
   - **Availability impact**—assess the degree of impact that the incident had on system availability:
     - **High**
     - **Low**
     - **None**
   - **Integrity impact**—assess the degree of impact that the incident had on system integrity:
     - **High**
     - **Low**
     - **None**

- **Confidentiality impact**—assess the degree of impact that the incident had on data confidentiality:
  - **High**
  - **Low**
  - **None**
- **Custom impact**—specify other significant impacts from the incident.
- **City**—indicate the city where your organization is located.

7. If assets are attached to the incident, you can specify their settings on the **Technical details** tab.

   This tab becomes active only if you select the **Affected system has internet connection** check box.

   If you need to edit or supplement the information previously specified on the **Technical details** tab, you should do this in your GosSOPKA account, even if NCIRCC experts requested additional information from you, and you can edit the exported incident.

   The categories of the listed assets must match the category of the affected CII in your system.

8. Click **Export**.

9. Confirm the export.

   Information about the incident is submitted to NCIRCC, and the **Export to NCIRCC** incident setting is changed to **Exported**. At NCIRCC, the incident received from you is assigned a registration number and status. This information is displayed in the incident window in the **NCIRCC integration** section.

It is possible to change the data in the exported incident only if the NCIRCC experts requested additional information from you. If no additional information was requested, but you need to update the exported incident, you should do it in your GosSOPKA dashboard.

After the incident is successfully exported, the **Compare KUMA incident to NCIRCC data** button is displayed at the bottom of the screen. When you click this button, a window opens, where the differences in the incident data between KUMA and NCIRCC are highlighted.

Getting incidents from NCIRCC

After upgrading to version 3.4.1, at each startup, KUMA Core sends a request to get new incident cards to the address specified in the URL field in KUMA's NCIRCC integration settings, and then continues sending requests every 10 minutes. If a new incident appears in the NCIRCC user account dashboard, KUMA registers the incident with the ALRT* prefix and further interaction with NCIRCC is carried out in context of the created incident.

Interaction with NCIRCC is available even if the incident in KUMA has the **Closed** status: you can edit the value of the **NCIRCC status** field and chat with NCIRCC.

Notifications about messages from NCIRCC are sent to the email addresses of users with the General administrator role.

Fields of a new incident are populated as shown in the following table.

Field values of an incident received from NCIRCC.

Field name	Value
Created by	When an incident is created in KUMA, creation date and time are automatically specified. Example: 2024-10-08 05:32:39
Name	ID or registration number of the incident (message) in GosSOPKA. Example: ALRT-xx-xx-xxx
Tenant	The tenant in which incidents received from NCIRCC must be created. By default, all incidents are created in the Main tenant. You can change the incident creation tenant in the NCIRCC integration settings. Example: Main.
Status	Initial status of the KUMA incident. Example: **Open**.
Severity	Degree of significance of the potential security threat. Default: **Critical**. Possible values: **Critical**, **High**, **Medium**, **Low**.
Affected asset categories	Empty. This value can be filled in manually.
First event time	Empty. This value can be filled in manually.
Last event time	Empty. This value can be filled in manually.
Description	The value from the event_description field of the message sent by NCIRCC. Can be edited. Example: message from NCIRCC.
Related tenants	Same as the Tenant field. Example: Main.
Available tenants	Same as the Tenant field. Example: Main.
Related alerts	Empty. This value can be filled in manually.
Related endpoints	Empty. This value can be filled in manually.
Related users	Empty. This value can be filled in manually.
Change log	Empty. This value can be filled in manually.
NCIRCC integration section	
Category	Category of the message card. Dictionary value. Possible values: Message from NCIRCC. This field is not editable.
Type	Type of the information security event. Value from the dictionary. Possible values: **Infected resource**, **Source of malware email messages**, **Source of malware modules**, **Malware operation center**, **Malware infrastructure element**, **Resource slowdown**, **Source of exploit**, **Source of user account compromise**, **Participant of network traffic capture**, **Source of unauthorized access**, **Source of unauthorized modification of information**, **Source of spam**, **Publication of information illegal in the Russian Federation**, **Hosting of a phishing resource**, **Unauthorized content**, **Participant of DDoS attack**, **Compromised user account**, **Network Scan Source**, **Participant of fraud**, **Source of social engineering threat**, **Vulnerable resource**, **Suspected phishing resource**, **Threat of personal data compromise**, **Threat of computer attack**. This field is not editable.
Status of export to NCIRCC	**Imported from NCIRCC**. This field is not editable.
NCIRCC message processing progress section	
NCIRCC status	NCIRCC message processing status. Value from the dictionary. This field is editable. Possible values: **New**, **In progress**, **Decision made**, **Interaction completed**, **Archived**.
Result	Result of the decision made. Value from the dictionary. This field is editable. Possible values: **Measures have been taken**, **Information taken into account**, **Information not confirmed**.
Chat with NCIRCC section	
UUID	Unique ID of the NCIRCC message.
Company	Short name of the GosSOPKA subject organization.
Category	Category of the message card. Dictionary value. Example: message from NCIRCC.
Type	Type of the information security event. Value from the dictionary. Example: infected resource.
Creation time	Date and time when the NCIRCC message was registered. Follows the ISO 8601 standard. UTC time is used.

Field name	Value
Time of detection	Date and time when the incident was detected. Follows the ISO 8601 standard. UTC time is used.
Incident end time	Date and time when the incident ended. Follows the ISO 8601 standard. UTC time is used.
Updated	Date and time when the message card was last updated. Follows the ISO 8601 standard. UTC time is used.
Event description	Brief description of the information security event. Up to 5000 Unicode characters.
Owner name	Owner of the information resource. Up to 5000 Unicode characters.
Incident ID in NCIRCC	Registration number of the message. Example: ALRT-20-12-2914.
TLP	TLP limitation marker. Dictionary value. Possible values: **TLP:WHITE**, **TLP:GREEN**, **TLP:AMBER**, **TLP:RED**.
Technical details section	
The **Technical details** group of fields is displayed with the field values obtained from the message. Which **NCIRCC message** fields are present in the **Technical details** group depends on the Information security event type, and the set of fields may differ depending on the incident. Pay close attention to the field values in your NCIRCC account. Values are not editable.	

Supplementing incident data on request

If NCIRCC experts need additional information about the incident, they may request it from you. In this case, the incident status changes to **More information required** in the **NCIRCC integration** section of the incident window. The following KUMA users receive email notifications about the status change: the user to whom the incident is assigned and the user who exported the incident to NCIRCC.

If an incident is assigned the *More information required* status in NCIRCC, the following actions are also available for this incident in KUMA:

- Upload files to NCIRCC.
- Re-export the incident data to NCIRCC with updates or additions to the previously provided information. This action completes supplementing the incident data.

Sending files to NCIRCC

You can attach a file to an incident if the incident has one of the following NCIRCC statuses: *New*, *In progress*, *More information required*, *Decision made*. The file will be available both in NCIRCC and in the KUMA web interface.

For a hierarchical deployment of KUMA, files can only be uploaded to NCIRCC from the parent KUMA node. At the same time, log entries about the file download are visible in the child nodes of KUMA.

In the incident change log, messages about the files uploaded to NCIRCC by KUMA users are added. Messages about adding files by NCIRCC are not added to the log.

To attach a file to an incident:

1. In the **Incidents** section of the KUMA web interface, open the incident you want to attach a file to.
2. In the **NCIRCC integration** section of the incident window, select the **File** tab and click the **Send file to NCIRCC** button.

   The file selection window opens.
3. Select the required file no larger than 50 MB and confirm your selection.

The file is attached to the incident and available for both NCIRCC experts and KUMA users.

Data in KUMA and NCIRCC is synchronized every 5-10 minutes.

Communication with NCIRCC experts

After the incident is successfully exported to NCIRCC, a chat with NCIRCC experts becomes available at the bottom of the screen. You can exchange messages since successful incident export to NCIRCC until it is closed in NCIRCC.

The chat window with the message history and the field for entering new messages is available on the **Chat** tab in the **NCIRCC integration** section of the incident window.

Data in KUMA and NCIRCC is synchronized every 5-10 minutes.

Supported categories and types of NCIRCC incidents

The table below lists the categories and types of incidents that can be exported to NCIRCC:

Incident category	Incident type
Computer incident notification	Slowed operation of the resource due to a DDoS attack
	Malware infection
	Network traffic interception
	Compromised user account
	Unauthorized data modification
	Unauthorized disclosure of information
	Publication of illegal information on the resource
	Successful exploitation of a vulnerability
	Event is not related to a computer attack
	Use of a controlled resource for attacks

Incident category	Incident type
Notification about a computer attack	DDoS attack
	Unsuccessful authorization attempts
	Malware injection attempts
	Attempts to exploit a vulnerability
	Publication of fraudulent information
	Network scanning
	Social engineering
Notification about a detected vulnerability	Vulnerable resource

Notifications about the incident status change in NCIRCC

In the event of certain changes in the status or data of an incident at NCIRCC, KUMA users receive the following notifications by email:

- Notification about receiving a message from NCIRCC.
- Additional data request notification.
- Notification about the incident status change in NCIRCC.
- Notification about automatic closure of an incident.

The following users receive notifications:

- The user to whom the incident was assigned.
- The user who exported the incident to NCIRCC.

Example of incident investigation using Kaspersky SIEM

Detecting an attack on the corporate IT infrastructure using Kaspersky SIEM solution includes the following steps:

1. Preliminary steps
2. Assigning an alert to a user
3. Check if the triggered correlation rule matches the data of the alert events
4. Analyzing alert information
5. False positive check
6. Determining alert severity
7. Incident creation
8. Investigation

9. Searching for related assets
10. Searching for related events
11. Recording the causes of the incident
12. Response
13. Restoring assets operability
14. Closing the incident

The description of the steps provides an example of response actions that an analyst might take when an incident is detected in the organization's IT infrastructure. You can view the description and example for each step by clicking the link in its title. The examples are directly relevant to the step being described.

For conditions of the incident for which examples are provided, see the *Incident conditions* section.

For more information about response methods and tools, see the *Incident Response Guide*. On the Securelist website by Kaspersky, you can also find additional recommendations for incident detection and response.

Incident conditions

Parameters of the computer (hereinafter also referred to as "asset") on which the incident occurred:

- Asset operating system – Windows 10.
- Asset software – Kaspersky Endpoint Agent, Kaspersky Endpoint Security.

KUMA settings:

- Integration with Active Directory, Kaspersky Security Center, Kaspersky Endpoint Detection and Response is configured.
- *SOC_package* correlation rules from the solution distribution kit are installed.

A cybercriminal noticed that the administrator's computer was not locked, and performed the following actions on this computer:

1. Uploaded a malicious file from his server.
2. Executed the command for creating a registry key in the `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` hive.
3. Added the file downloaded at the first step to autorun using the registry.
4. Cleared the Windows Security Event Log.
5. Completed the session.

Step 1. Preliminary steps

Preliminary steps are as follows:

1. Event monitoring.

   When a collector is created and configured in KUMA, the solution writes information security events registered on controlled elements of the organization's IT infrastructure to the event database. You can find and view these events.

2. Creating a correlator and correlation rules.

   When a sequence of events that satisfy the conditions of a correlation rule is detected, the solution generates alerts. If the same correlation rule is triggered for several events, all these events are associated with the same alert. You can use correlation rules from the distribution kit or create them manually.

3. Configuring email notifications about an alert to one or more email addresses.

   If notification is configured, KUMA sends a notification to the specified email addresses when a new alert is received. The alert link is displayed in the notification.

4. Adding assets.

   You can only perform response actions for an asset (for example, block a file from running) if the asset is added to KUMA.

   Performing response action requires integrating KUMA with Kaspersky Security Center and Kaspersky Endpoint Detection and Response.

   Example
   The analyst has carried out the following preliminary steps:

   - Installed the *SOC_package* correlation rules from the distribution kit and linked them to the correlator.
   - Configured the sending of alert notifications to the analyst's email.
   - Imported assets from Kaspersky Security Center to KUMA.

   According to the incident conditions, after the administrator logged into their account, a malicious file was run, which the attacker had added to Windows autorun. The asset sent Windows security event log events to KUMA. The correlation rules were triggered for these events.

   As a result, the following alerts were written to the KUMA alert database:

   - R223_Collection of information about processes.
   - R050_Windows Event Log was cleared. R295_System manipulations by a non-privileged process.
   - R097_Startup script manipulation.
   - R093_Modification of critical registry hives.

   The information about the alert contains the names of the correlation rules based on which the alerts were created, and the time of the first and last event created when the rules were triggered again.

   The analyst received alert notifications by email. The analyst followed the link to the *R093_Changes to critical registry hives* alert from the notification.

Step 2. Assigning an alert to a user

You can assign an alert to yourself or to another user.

Example
As part of the incident, the analyst assigns the alert to themselves.

Step 3. Check if the triggered correlation rule matches the data of the alert events

At this step, you must view the information about the alert and make sure that the alert event data matches the triggered correlation rule.

Example
The name of the alert indicates that a critical registry hive was modified. The **Related events** section of the alert details displays the table of events related to the alert. The analyst sees that the table contains one event showing the path to the modified registry key, as well as the original and the new value of the key. Therefore, the correlation rule matches the event.

Step 4. Analyzing alert information

At this step, analyze the information about the alert to determine what data is required for further analysis of the alert.

Example
From the alert information, the analyst learns the following:

- Which registry key has been modified
- On which asset
- The name of the account used to modify the key

This information can be viewed in the details of the event that caused the alert (**Alerts** → *R093_Modification of critical registry hives* → **Related events** → event 2022-08-23 17:27:05), in the FileName, DeviceHostName, and SourceUserName fields respectively.

Step 5. False positive check

At this stage, make sure that the activity that triggered the correlation rule is abnormal for the organization IT infrastructure.

Example
At this step, the analyst checks whether the detected activity can be legitimate as part of normal system operation (for example, an update). The event information shows that a registry key was created under the user account using the *reg.exe* utility. A registry key was also created in the `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` hive, responsible for autorun of applications at user logon. Based on this information, one can surmise that the activity is not legitimate and the alarm is not false.

Step 6. Determining alert severity

You can change the alert severity level, if necessary.

Example
The analyst assigns a high severity to the alert.

Step 7. Incident creation

If steps 3 to 6 reveal that the alert warrants investigation, you can create an incident.

Example
The analyst creates an incident in order to perform an investigation.

Step 8. Investigation

This step includes viewing information about the assets, accounts, and alerts related to the incident in the incident information section.

Information about the impacted assets and accounts is displayed on the **Related assets** and **Related users** tabs in the incident information section.

Example
The analyst opens the information about the affected asset (**Incidents** → the relevant incident → **Related alerts** → the relevant alert → **Related endpoints** → the relevant asset). The asset information shows that the asset belongs to the *Business impact/HIGH* and *Device type/Workstation* categories, which are critical for the organization IT infrastructure.

The asset information also includes the following useful data:

- FQDN, IP address, and MAC address of the asset.
- The time when the asset was created and the information was last updated.
- The number of alerts associated with this asset.
- The categories to which the asset belongs.
- Asset vulnerabilities.
- Information about the installed software.
- Information about the hardware characteristics of the asset.

The analyst opens the information about the associated user account (**Incidents** → the relevant incident → **Related alerts** → link with the relevant alert → **Related users** → account).

The following account information may be useful:

- User name.
- Account name.
- Email address.
- Groups the account belongs to.
- Password expiration date.
- Password creation date.
- Time of the last invalid password entry.

Step 9. Searching for related assets

You can view the alerts that occurred on the assets related to the incident.

Example
The analyst checks for other alerts that occurred on the assets related to the incident (**Incidents** → the relevant incident → **Related alerts** → the relevant alert → **Related endpoints** → the relevant asset → **Related alerts**). In the alert window, you can configure filtering by time or status to exclude outdated and processed alerts. The time when the asset alerts were registered helps the analyst to determine that these alerts are related, so they can be linked to the incident (select the relevant alerts → **Link** → the relevant incident → **Link**).

The analyst also finds the associated alerts for the account and links them to the incident. All related assets that were mentioned in the new alerts are also scanned.

Step 10. Searching for related events

You can expand your investigation scope by searching for events of related alerts.

The events can be found in the KUMA event database manually or by selecting any of the related alerts and clicking **Find in events** in the alert details (**Incidents** → the relevant incident → **Related alerts** → the relevant alert → **Related endpoints** → **Find in events**). The found events can be linked to the selected alert, however, the alert must be unlinked from the incident before that.

Example

As a result, the analyst found the *A new process has been created* event, where the command to create a new registry key was recorded. Based on the event data, the analyst detected that `cmd.exe` was the parent process for `reg.exe`. In other words, the cybercriminal started the command line and executed the command in it. The event details include information about the *ChromeUpdate.bat* file that was autorun. To find out the origin of this file, the analyst searched for events in the event database using the `FileName = ‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’` field and the `%%4417` access mask (access type *WriteData (or AddFile)*):

```
SELECT * FROM 'events' WHERE DeviceCustomString1 like '%4417%' and FileName like
‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’ AND Device Vendor 'Microsoft' ORDER BY Timestamp DESC LIMIT 250
```

As a result, the analyst discovered that the file was downloaded from an external source using the `msedge.exe process.` The analyst linked this event to the alert as well.

Search for the related events for each incident alert allows the analyst to identify the entire attack chain.

Step 11. Recording the causes of the incident

You can record the information necessary for the investigation in the incident change log.

Example

Based on the results of the search for incident-related events, the analyst identified the causes of the incident and recorded the results of the analysis in the **Change log** field in incident details to pass the information to other analysts.

Step 12. Incident response

You can perform the following response actions:

1. Isolate the asset from the network.
2. Perform a virus scan.
3. Prevent the file from running on assets.

> The listed actions are available if KUMA is integrated with Kaspersky Security Center and Kaspersky Endpoint Detection and Response.

Example
The analyst has information about the incident-related assets and the indicators of compromise. This information helps select the response actions.

As part of the incident being considered, it is recommended to perform the following actions:

- Start an unscheduled virus scan of the asset where the file was added to autorun.
  The virus scan task is started by means of Kaspersky Security Center.
- Isolate the asset from the network for the period of the virus scan.
  The asset isolation is performed by means of Kaspersky Endpoint Detection and Response.
- Quarantine the *ChromeUpdate.bat* file and create the execution prevention rules for this file on other assets in the organization.
  An execution prevention rule for a file is created by means of Kaspersky Endpoint Detection and Response.

Step 13. Restoring assets operability

After the IT infrastructure is cleaned from the malicious presence, you can disable the prevention rules and asset network isolation rules in Kaspersky Endpoint Detection and Response.

Example
After the investigation, response, and cleanup of the organization IT infrastructure from the traces of the attack, restoration of the asset operation can be started. For this purpose, the execution prevention rules and the network asset isolation rules can be disabled in Kaspersky Endpoint Detection and Response if they were not disabled automatically.

Step 14. Closing the incident

After taking measures to clean up the traces of the attacker's presence from the organization's IT infrastructure, you can close the incident.

AI services

This section provides information about the AI services that KUMA works with.

AI score and status of assets

The **AI asset score and status** service (hereinafter also referred to as the AI service) allows you to clarify the severity of correlation events generated by triggered correlation rules. The AI service can be installed if your license covers the AI module.

The AI service gets correlation events with a non-empty **Affected assets** field from the available storage clusters, constructs the expected sequence of events, and trains the AI model. Based on the chain of triggered correlation rules, the AI service calculates whether such a sequence of events is typical for this infrastructure. The AI service calculates the AI score and the AI status, which become available in the asset card. Non-typical patterns increase the score of the asset.

The *asset score* is a number that quantifies how non-typical the activity is, and whether it is worth paying attention to. The score is assigned as follows:

- **Low**: 0 ≤ score < 0.25
- **Medium**: 0.25 ≤ score < 0.5

- **High**: 0.5 ≤ score < 0.75
- **Critical**: 0.75 ≤ score ≤ 1

Every time the AI service is restarted, it trains the model from scratch and reassesses the score of the assets mentioned in events of the current day. The model is retrained at midnight UTC. The asset score is reassessed once an hour for all assets that were mentioned in events of the current day (UTC).

If you remove the license key, the **Score AI** and **Status AI** fields are hidden from the asset card. When you add a license key, the values of **Score AI** and **Status AI** fields are displayed again.

The **Assets by severity** widget allows tracking the distribution of assets by status. This widget is available if your license covers the AI module. The pie chart indicates the numbers of assets grouped by status.

You can apply a filter by the **Score AI** and **Status AI** fields when searching for assets. You can also set up proactive asset categorization by **Score AI** and **Status AI** fields. In this case, as soon as the AI service assigns a rating to an asset, the asset is moved to the category specified for this level of risk. You can create a structure of multiple categories and automatically populate these with assets in accordance with the calculated risk values.

If necessary, you can configure audit events to be generated when an asset is added to a category. Audit events can be taken into account in correlation rules, and you can monitor them on the dashboard and in reports.

To track changes of asset categories in the dashboard, you need to create an **Events** widget with the following query:

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value` FROM `events`
where DeviceVendor = 'Kaspersky' and DeviceProduct = 'KUMA' and
DeviceEventCategory = 'Audit assets' and DeviceAction= 'asset added to category'
and DeviceCustomString1 = 'Main/Categorized assets/ML/score>0.5'
GROUP BY Timestamp ORDER BY value LIMIT 250
```

The directory specified in the configuration file stores events that the AI service got from KUMA storage clusters for the specified number of days. For example, if the configuration file specifies 12 days, the AI service gets events for the past 12 days. The oldest events are deleted from the directory. The trained model is stored in the same directory.

Service logs are stored in the `/var/log/syslog` directory.

Installing and removing the AI asset score and status service

Installing the AI asset score and status service

To install the service:

1. Extract the `mlservice-installer-XX.tgz` archive that is included in the distribution kit.

   The `mlservice-installer-XX.tgz` archive contains scripts for installing and removing the service, as well as the `config.yaml` configuration file.

2. In the `config.yaml` configuration file, in the `kuma_address` setting, specify the FQDN of the host on which KUMA Core is installed and the port on which the KUMA Core is to listen for AI service connections.

To install in a high availability configuration, specify port 7226. You can keep default values for the rest of the settings.

After installation, the AI service starts with the settings specified in the `config.yaml` file.

3. If you want to install the service on a remote host, specify the address of the remote host in the `inventory.yaml` file and make sure you have network access.

   By default, the service is installed on the local host as specified in `inventory.yaml`.

4. Get the KUMA Core certificate. To do this, in the web interface, click the name of your user account and in the displayed menu, select **AI service certificate**.

   The certificate is downloaded to your default download directory.

   If necessary, you can reissue the AI service certificate.

5. Save the KUMA Core certificate file in the `roles/mlservice/files` directory under the installer directory.

6. Change to the directory with the service files and from that directory, run the following command:

```
./install <path to inventory.yaml>
```

7. Read the terms of the End User License Agreement.

   If you accept the terms and conditions of the End User License Agreement, press `Y`. If you do not accept the terms and conditions of the End User License Agreement, you cannot proceed with the installation of the service.

   You can find the file with the text of the End User License Agreement in the `mlservice-installer/eula` directory.

8. The installer generates a certificate and a key during the installation process and places these in the directories specified in the `config.yaml` configuration file. Upload the certificate to KUMA.

   In the web interface, open the **Settings** → **Integrations** → **AI services** section, and in the **AI asset score and status** window, fill in the following fields:

   a. In the **URL** field, specify the FQDN of the KUMA Core host on and the port on which the KUMA Core listens for the AI service, for example: `<FQDN of the KUMA Core host>:7226`.

      The port number must match the port number specified in the configuration file. Make sure the port is not being used by other applications.

      For a high-availability installation of KUMA, the **URL** field is not displayed in the web interface. The port value is taken from the `KUMA_APPRAISER_AI_API_PORT` environment variable, and the port is opened for all IP addresses of the KUMA Core host.

   b. In the **Certificate** field, select **Create new** from the drop-down list. This opens the **Create secret** window; in that window, specify the **Certificate** type of secret and upload the certificate from the directory specified in the `config.yaml` configuration file.

   c. Enable the **State** toggle switch. The toggle switch is disabled by default.

   d. Click **Save**.

   Immediately after installation, the service will make attempts to connect to KUMA for 15 minutes with 1-minute intervals. If no certificate is added in the KUMA web interface, the connection will fail and the service will stop. In this case, add a certificate and restart the AI service; the service makes new attempts to connect.

   After saving the settings, get the log of the KUMA Core server and make sure it does not contain the `<port number>: bind: address already in use` error

The AI service is installed.

Removing the AI asset score and status service

To remove the AI service:

1. Go to the directory with the AI service files.
2. In this directory, run the following command:

```
./uninstall <path to inventory.yaml>
```

Settings of the AI asset score and status service

The table below describes the settings for the AI service.

AI service settings

Setting	Description
`cert_file_path`	Path to the directory that contains the certificate generated by the installer. Default path: `/opt/kaspersky/mlservice/service.crt` You can specify a different path. In this case, make sure that the user that starts the service has access to the specified directory.
`key_file_path`	Path to the directory that contains the key generated by the installer. Default path: `/opt/kaspersky/mlservice/service.key` You can specify a different path. In this case, make sure that the user that starts the service has access to the specified directory.
`kuma_address`	FQDN of the host on which the KUMA Core is installed and port on which the KUMA Core is to listen for the AI service. To install in a high availability configuration, specify port 7226. Example <FQDN of the host on which KUMA Core is installed>:7226
`kuma_cert_file_path`	Path to the directory where the KUMA Core certificate is located. Default path: `/opt/kaspersky/mlservice/core-external-ca.cert`
`event_storage_path`	Path to the directory where the service is to place received correlation events. Default path: `/var/mlservice/events`
`model_storage_path`	Path to the directory where the service is to place the trained model. Default path: `/var/mlservice/models`
`period_for_train_days`	The number of days for which you want to get correlation events that involve your assets from the available storage clusters in order to train the model. The default setting is 12 days. This means that the directory will contain events for the past <N> days. The oldest events are deleted.

Setting	Description
`events_overlap_in_seconds`	Overlap time. When events for assessing the scores of assets are downloaded on a schedule, they are retrieved from the time of the last downloaded event for the current day minus the value of the `events_overlap_in_seconds` setting. The default value is 60 seconds. Example: the time when the last event was received is 8:58. The starting time for the next batch of events to be downloaded is 8:57.

Using the KIRA AI Assistant

Attackers use command coding and obfuscation to conceal their actions as much as possible. You can use Kaspersky Investigation and Response Assistant AI-assistant (hereinafter also referred to as KIRA) to remove deobfuscation, receive step-by-step explanation of what happens if you execute such command, and determine the level of risk of executing this command. KIRA helps to quickly investigate alerts and incidents, and also reduces the likelihood of error in the analysis.

You can analyze a command using KIRA if, during normalization, the command enters the event field. The analysis results are kept in cache for 14 days and are available for review. An audit event is generated on each request.

You can configure integration with KIRA in one of the following ways:

- Using the Kaspersky Security Network (**KSN** mode), when a request is sent through the Kaspersky cloud service.
- Using a third-party LLM provider (**Custom** mode), when the request is sent directly to the specified API.

  The provider, model, and parameter configuration are selected by the user. Data processing is performed by the selected service.

  KUMA supports the following third-party LLM providers:

  - GPT-5.4
  - Deepseek-V4-Pro
  - Kimi K2.6
  - GLM-5.1
  - MiniMax M2.7

KIRA is available in the RU region if the following conditions are satisfied:

- There is a current license covering the AI module.

  If the license has expired, the analysis results remain available via tasks for 14 days from the moment a result is cached.
- A certificate was uploaded when configuring the KIRA integration using KSN. You can get the certificate file in PFX format packed in the `<customer name>.ZIP` archive and the password for the certificate from Technical Support.
- When configuring integration with KIRA using a third-party LLM provider, a connection to the provider's API is configured.

- The user has one of the following roles with corresponding access rights: Main administrator, Administrator, Tier 2 analyst, Tier 1 analyst, and Junior analyst.

  Only a user with the General administrator role can configure the integration.

Configuring integration with KIRA using KSN

To configure integration with KIRA via KSN:

1. Get a license with the AI module and activate the functionality in KUMA.
2. In the web interface, open the **Settings** → **Integrations** → **AI Services** section.
3. This opens a window; in that window, go to the **Kaspersky Investigation & Response Assistant** tab.
4. Enable KIRA integration by enabling the **State** toggle switch.

   The toggle switch is turned off by default.
5. Under **Mode**, select the **KSN** operation mode.
6. Click **Select file** and download the `<customer name>.ZIP` archive, which contains the certificate in PFX format.
7. In the **Certificate password**, enter the password.
8. In the **Proxy server** drop-down list, select or create a proxy server.
9. In the drop-down list, select the KIRA response language, Russian or English.

   KUMA sends and stores KIRA responses in the language of your choice.

   Russian is selected by default.
10. Click **Save**.

    After clicking **Save**, you are prompted to accept the terms and conditions of the End Use License Agreement. If you do not accept the End Use License Agreement, you won't be able to save the settings or continue to use KIRA.

    After saving the settings, the available number of tokens is displayed. The tokens are replenished every day.

Integration is configured, you can proceed to the analysis. Analysis is available for all events: new and previously received.

Configuring integration with KIRA using an LLM provider

For a visual demonstration of how to configure integration using an LLM provider, you can watch the video below.

To configure KIRA integration using a third-party LLM provider:

1. Get a license with the AI module and activate the functionality in KUMA.
2. In the web interface, open the **Settings** → **Integrations** → **AI Services** section.
3. This opens a window; in that window, go to the **Kaspersky Investigation & Response Assistant** tab.
4. Enable integration with KIRA by enabling the **Status** toggle switch.

   The toggle switch is turned off by default.
5. Under **Mode**, select the **Other** mode of interaction with KIRA.

   By default, the **KSN** mode is selected.
6. In the "**Base URL**" field, enter the provider's API address (for example, `https://api.openai.com/v1`). The address must start with `http://` or `https://`.
7. In the **API key** drop-down list, select or create a secret of the **token** type.

   How to create a secret

   To create a secret:

   1. In the **Name** field, enter the name of the secret.
   2. In the **User** and **Password** fields, enter the credentials of the user account that the Agent will use to connect to the connector.
   3. If necessary, enter a description of the secret in the **Description** field.
   4. Then click the **Create** button.

   The secret is added and displayed in the **Secret** drop-down list.

If the API that you are using does not require a key, in the **API key** field, specify a secret with the **api-key** value.

8. In the "**Model**" field, specify the name of the model that your provider uses (for example, `gpt-4-turbo`, `llama3-70b`).

9. In the **Maximum prompt size** field, specify the maximum number of tokens in a request.

10. In the **Proxy server** drop-down list, select or create a proxy server.

11. Select the KIRA response language, Russian or English.

    KUMA sends and stores KIRA responses in the language of your choice.

    Russian is selected by default.

12. Click the **Add JSON file** button to upload a file with the model parameters and HTTP headers.

    In this file, you can specify additional parameters of the request to the LLM provider (for example, `temperature`, `max_tokens`). You can also specify additional HTTP headers. To do this, you need to use the `"headers"` key. If multiple `"headers"` keys are specified in the file, only the first of those is used.

    Example of file content

    ```
    {
      "temperature": 0.5,
      "max_tokens": 20000,
      "headers": {
        "OpenAI-Organization": "ORG_ID"
      }
    }
    ```

    The AI service returns an error if at least one of the following parameters is specified in the JSON file: `messages`, `model`, `audio`, `function_call`, `functions`, `modalities`, `n`, `parallel_tool_calls`, `prediction`, `response_format`, `stop`, `stream`, `stream_options`, `tool_choice`, `tools`, `web_search_options`.

13. Click **Test connection** to make a test request to the specified API.

14. Click **Save**.

    After clicking **Save**, you are prompted to accept the terms and conditions of the End Use License Agreement. If you do not accept the End Use License Agreement, you won't be able to save the settings or continue to use KIRA.

    After saving the settings, the available number of tokens is displayed. The tokens are replenished every day.

Integration is configured, you can proceed to the analysis. Analysis is available for all events: new and previously received.

Analyzing using KIRA

After configuring the integration, you can analyze commands using KIRA.

To learn more about analysis using KIRA, watch this video:

To perform an analysis:

1. Open the details of the event or correlation event.

2. In the toolbar, in the **Analyze with KIRA** drop-down list, select the field whose value you want to analyze.

   This opens the **Analyze with KIRA** window, displaying the command to be analysed.

3. If necessary, follow one of these steps:

   - By default, an obfuscated command is automatically deobfuscated without spending tokens. If you want to analyze the command in its original obfuscated form, in the **Actions** drop-down list, select **Revert to original string**. Deobfuscate the string again if necessary.

   - If you want to know in advance how many tokens will be spent on analysis, in the **Actions** drop-down list, select **Calculate size in tokens**.

     Number of tokens for analysis = number of tokens to send a request + number of tokens to produce a response.

4. To analyze the command, click the **Analyze** button.

   If you have enough tokens, the analysis and the **Query to KIRA task** are started. Processing the request may take 30 seconds or longer.

   The information on the available number of tokens is also updated. Tokens are consumed even if an error is received indicating that the requested topic is on the denylist.

The command is analyzed. The output, summary, and detailed analysis are available in the **Analyze with KIRA** window.

The analysis result using KIRA can also be viewed in a separate window. To do this, click **View result** in the displayed notification. The **KIRA result** window opens. You can click **Go to event** link in this window to open the corresponding event.

In the event details, the analysis result is displayed on the **KIRA analysis** tab and is available to all users with access to the **Analyze with KIRA** functionality.

The analysis result is also available in the **Task Manager** section in the properties of the **Query to KIRA** task. You can click the name of the task and select one of the following options in the context menu:

- **View result**: if you have access to KIRA tasks, the results of the analysis are displayed. In this case, tokens are not used.
- **Restart**: the analysis is performed without taking into account the data of the previous analysis; in this case, the analysis costs tokens.

The table below lists possible errors when performing the analysis.

Errors of the Analyze with KIRA task

HTTP code	Description
400	Invalid client certificate.
404	Error in request.
401	Missing certificate information. Contact Technical Support.
403	The number of tokens available per day was exceeded.
413	Maximum number of tokens for request reached. Make the request smaller.
500	Unknown error of the service.
502	KIRA service unavailable.
503	Error getting access token in service.
Other	Unknown error.
No code	Error while processing the request.

DLL Hijacking attack detection

DLL Hijacking is an attack technique that involves delivering vulnerable legitimate software along with a malicious dynamic link library (DLL) to the target system. When the vulnerable software is started, it does not verify whether the dynamic library is legitimate and loads it by file name, which results in the execution of malicious code. A DLL Hijacking attack is difficult to detect because the software being launched is in fact legitimate.

DLL Hijacking attacks are detected using the AI module, which analyzes how applications start and run and identifies suspicious cases of legitimate software running with malicious libraries. To configure the AI module, when creating an enrichment rule, select the **DLL Hijacking** type and then link it either to a collector or to a correlator. We recommend linking enrichment of this type to a correlator instead of a collector because a correlator scans correlation events while a collector scans base events. There are much fewer correlation events than base events, so much fewer queries are needed to check correlation events. Thus, the load on the KSN service is significantly lower when scanning events at a correlator than when scanning at a collector.

To get a status, KUMA sends a request to KSN. The request contains information from the event fields that is needed for analysis. In response to a request, KSN sends one of the following verdicts:

- `0` – **Unclassified**. To get a status, you need to re-send the request. You can configure the re-sending of requests using the **Perform a repeat request** setting.
- `1` – **Unknown**. The library is not considered malicious at the time when the status is received.

- 2 – **Suspicious**. Getting such a verdict creates an alert if you have the corresponding correlation rule configured.
- 3 – **Bad**. Getting such a verdict creates an alert if you have the corresponding correlation rule configured. The **Bad** status represents a higher-likelihood detection of DLL Hijacking than the **Suspicious** status.

The result is written to the KL_AI_DLLHijackingCheckResult field of the event as a numerical value and a text comment.

> To use an enrichment of the **check DLL Hijacking** type, your license must include the AI module. The General administrator needs also to accept the additional KSN Statement in the **Kaspersky Security Network** section (**Settings** → **Integrations** → **AI services** → **DLL Hijacking detection**). If your instance of KUMA has multiple General administrators, it is sufficient for one of them to accept the KSN Statement.

If there is no license or the license with the AI module has expired:

- You cannot create enrichment rules of the **DLL Hijacking** type. However, previously created rules remain viewable and also remain editable for seven days.
- The KL_AI_DLLHijackingCheckResult field remains viewable. You can also search and filter by this field.
- Collectors do not send requests for previously configured enrichments of the **DLL Hijacking** type.

Detecting DLL Hijacking attacks using event enrichment in the correlator

To configure DLL Hijacking attack detection using event enrichment in the correlator:

1. In the solution web interface, open the **Resources** → **Correlators** section.
2. Start creating a correlator or open the settings of an existing correlator.
3. Add an enrichment rule of the **check DLL Hijacking** type.

   When configuring enrichment, you need to fill in the following fields:

   - **dll hash (md5)**

     For example, if the DLL hash is in the `DeviceCustomString2` field, you need to map `DeviceCustomString2` <> **dll hash (md5)**.
   - **dll path**
   - **process hash (md5)**
   - **process path**
   - **process signature** and **dll size** if you want to improve the accuracy of DLL Hijacking attack detection.

   Such data is contained in "Module load" events of Kaspersky EDR Expert, in events of Sysmon Event ID 7.

   Make sure the fields you specify are populated as part of normalization in the collector. We recommend using the [OOTB] KEDR Telemetry normalizer imported from the repository.

4. In the **Correlation** section, create a simple or standard correlation rule. In the correlation rule, specify the same fields that you specified when adding the enrichment. If you created a simple correlation rule, the fields must be listed in the **Propagated fields** setting. For a standard correlation rule, the fields are listed in the **Identical fields** setting.

5. In the enrichment settings, in the list under **Filter parameters**, select the following filter: **[OOTB] Events for DLLHijacking enrichment. Filter for correlator**. If this filter is missing from the list, import it from the repository. You can also configure the filter on your own.

6. If you want to configure the solution to generate an alert when it gets a **Suspicious** or **Bad** verdict, create a correlation rule. When creating the correlation rule, select the simple or standard type and on the **Selector** tab, specify two conditions in the filter parameters:

```
Create an alert for the Suspicious verdict

KL_AI_DLLHijackingCheckResult = 2
```

```
Create an alert for the Bad verdict

KL_AI_DLLHijackingCheckResult = 3
```

DLL Hijacking attack detection is configured. If you have created a correlation rule, an alert is generated when a **Suspicious** or **Bad** verdict is received.

Detecting DLL Hijacking attacks using event enrichment in the collector

> We do not recommend using the **DLL Hijacking** enrichment in the collector. This increases the load on the KSN service. Instead, link an enrichment of this type to the correlator.

To configure DLL Hijacking attack detection using event enrichment in the collector:

1. In the solution web interface, open the **Resources** → **Collectors** section.

2. Start creating a collector or open the settings of an existing collector.

3. Add enrichment of the **Check DLL Hijacking** type.

   When configuring enrichment, you need to fill in the following fields:

   - **dll hash (md5)**

     For example, if the DLL hash is in the `DeviceCustomString2` field, you need to map `DeviceCustomString2` <> **dll hash (md5)**.

   - **dll path**

   - **process hash (md5)**

   - **process path**

   - **process signature** and **dll size** if you want to improve the accuracy of DLL Hijacking attack detection.

   Such data is contained in "Module load" events of Kaspersky EDR Expert, in events of Sysmon Event ID 7.

Make sure the fields you specify are populated as part of normalization in the collector.

4. In the enrichment settings, in the list under **Filter parameters**, select the following filter: **[OOTB] Events for DLLHijacking enrichment. Filter for collector**. If this filter is missing from the list, import it from the repository. You can also configure the filter on your own.

5. If you want to configure the solution to generate an alert when it gets a **Suspicious** or **Bad** verdict, create a correlation rule that does that. When creating the correlation rule, select the simple or standard type and on the **Selector** tab, specify two conditions in the filter parameters:

```
Create an alert for the Suspicious verdict

KL_AI_DLLHijackingCheckResult = 2
```

```
Create an alert for the Bad verdict

KL_AI_DLLHijackingCheckResult = 3
```

DLL Hijacking attack detection is configured. If you have created a correlation rule, an alert is generated when a **Suspicious** or **Bad** status is received.

Working with the task manager

When managing the solution web interface, you can use tasks to perform various operations. For example, you can import assets or export KUMA event information to a TSV file.

You can run multiple tasks at the same time. If you run tasks of different types, they are executed in parallel within the same tenant. Tasks of the same type can be run simultaneously only if the tenants are different. If you try to run multiple tasks of the same type in one tenant, only the first such task is run.

Viewing the tasks table

The tasks table contains a list of created tasks and is located in the **Task manager** section of the solution web interface window.

The ability to view other users' tasks depends on the user role. A user with the General administrator role can view the tasks of all users. Users with roles that allow reading and editing shared resources do not have access to tasks. Users with other roles, including users with the Tenant administrator role, can view all tasks in tenants available to them.

By default, the **View just mine** check box is selected in the **Task manager** section. To view all tasks, clear this check box.

The tasks table contains the following information:

- **State**—the state of the task. One of the following statuses can be assigned to a task:

  - **Running**—the task is active.

    You can stop a task of the **Run query in background** type in the **Running** status by clicking the **Stop and start in events** button. Clicking this button and confirming the action opens the **Events** section, where the query is run in normal mode.

- **Completed**—the task is complete.
- **Cancel**—the task was canceled by the user.
- **Error**—the task was not completed because of an error. The error message is displayed if you hover the mouse over the exclamation mark icon.

- **Task**—the task type. The solution provides the following types of tasks:
  - **Events export** exports KUMA events.
  - **Run query in background** runs an SQL query in the background.
  - **Retrospective scan** scans historical events.
  - **Threat Lookup** requests data from the Kaspersky Threat Intelligence Portal.
  - **KSC assets import** imports asset information from Kaspersky Security Center servers.
  - **KSC assets attributes import** imports information about the attributes of Kaspersky Security Center assets.
  - **KICS/KATA assets import** imports asset information from KICS/KATA.
  - **Accounts import** imports user information from Active Directory.
  - **Run program via KEDR**—starts an arbitrary application using Kaspersky Endpoint Detection and Response.
  - **Repository update**—updates the KUMA repository to receive the resource packages from the source specified in settings of the source.
  - **Update monitoring policies** updates the monitoring policy settings.
  - **Clearing resource change history** deletes information about resource changes.
  - **Export event sources** exports event sources in CSV format.
  - **Query to KIRA** requests an analysis of the command using Kaspersky Investigation & Response Assistant.
  - **Partition backup** is the task of backing up partitions according to a schedule or manually.
  - **Restoring partitions from backup** restores partitions from a backup copy.
  - **Importing partitions** imports partitions from an external KUMA installation.
- **Created by**—the user who created the task. If the task was created automatically, the column will show **Scheduled task**.
- **Created**—the date and time when the task was created.
- **Last updated**—date and time of the last update of the task.
- **Tenant**—the name of the tenant in which the task was started.

Configuring the display of the tasks table

You can customize the display of columns and the order in which they appear in the tasks table.

To customize the display in the task table:

1. In the KUMA web interface, select the **Task manager** section.

   The tasks table is displayed.

2. In the table header, click the gear (⚙) icon.

3. In the pane that is displayed:

   - If you want to enable display of a column in the table, select the check box next to the name of the parameter that you want to display in the table.

   - If you do not want the parameter to be displayed in the table, clear the check box.

   At least one check box must be selected.

4. If you want to reset the settings, click the **Default** link.

5. If you want to change the order in which the columns are displayed in the table, move the mouse cursor over the name of the column, hold down the left mouse button and drag the column to the necessary position.

The display of columns in the tasks table will be configured.

Viewing task run results

To view the results of a task:

1. In the KUMA web interface, select the **Task manager** section.

   The tasks table is displayed.

2. Do one of the following:

   - For tasks of the **Events export** and **Export event sources** type, click the link with the task type in the **Task** column and select **Download**.

     Task results are downloaded as a TSV file.

   - For tasks of the **Run query in background** type, click the task type link in the **Task** column. This opens the **Events** section in a new browser tab with the result of the SQL query.

   - Click the name of the user that created the task or **Scheduled task** in the **Created by** column.

     Task results are displayed in the sidebar.

For **Repository update** tasks, results are not displayed.

The presentation of task results in KUMA depend on the type of the task. For example, for **Threat Lookup**, information about the type of the detected object is displayed along with information about the file, detections, and access paths is displayed. For **KSC assets import** and **KICS/KATA assets import** tasks, information about the tenant and the number of downloaded objects is displayed. For the **Query to KIRA** task, information about task status, the date when the query was sent and the response received, and a link to the event are displayed.

In this section, the **View just mine** check box in the **Created by** column is selected by default. To view all tasks, clear this check box.

Restarting a task

To restart a task:

1. In the KUMA web interface, select the **Task manager** section.

   The tasks table is displayed.

2. Select the check box next to the task you want to restart.

3. Click the **Restart** button.

The task will be restarted.

Troubleshooting

This section lists solutions to several common problems that you may encounter when using KUMA.

If necessary, see also the Troubleshooting section in the Knowledge Base.

Known issues and limitations

KUMA has some limitations that are not critical for the operation of the application:

- After upgrading KUMA 3.4 to version 4.0, some widgets on the dashboard are displayed with an error. To fix the error, please manually refresh the data on the dashboard or wait for it to be refreshed automatically.
- The widget form can be opened below the **Dashboards** settings form when you follow links from the **Used in widgets** column if you have opened the settings of any widget before opening the **Dashboards** settings form.
- In KUMA 4.6, correlation rules of the **periodical** type cannot be created in the NG correlator.

Contact Technical Support

If you did not find a solution to your problem in the documentation or other sources of information about KUMA, we recommend contacting Technical Support. Our Technical Support team will answer your questions about installing and using KUMA.

> Kaspersky provides support for KUMA throughout its lifecycle (see the solution lifecycle page). Before contacting Technical Support, please read the technical support rules.

You can contact Technical Support in one of the following ways:

- By visiting the Technical Support website
- By submitting a request to Kaspersky Technical Support from the Kaspersky CompanyAccount portal.

When processing your request, Kaspersky Technical Support may need a report generated by the collect.sh utility. For detailed information on using the utility, please refer to the Knowledge Base.

KUMA logs

KUMA provides the following types of logs:

- Installer logs
- Component logs

You can also generate a report with diagnostic information about your device using the `collect.sh` utility. For detailed information on using the utility, please refer to the Knowledge Base.

Installer logs

KUMA automatically creates files containing logs of installation, reconfiguration, or removal.

The logs are stored in the `./log/` directory in the installer directory. The name of the log file reflects the date and time when the corresponding script was started.

Names are generated in the following formats:

- Installation log: `install-YYYYMMDD-HHMMSS.log`. For example: `install-20231031-102409.log`.
- Removal logs: `uninstall-YYYYMMDD-HHMMSS.log`. For example: `uninstall-20231031-134011.log`.
- Reconfiguration logs: `expand-YYYYMMDD-HHMMSS.log`. For example: `expand-20231031-105805.log`.

The solution creates a new log file each time an installation, reconfiguration, or removal script is started. Log rotation or automatic deletion is not performed.

The log incorporates the lines of the inventory file used when the corresponding command was invoked, and the ansible log. For each task, the following information is listed in this order: task start time (Tuesday, October 31, 2023 10:29:14 +0300), run time of the previous task (0:00:02.611), and the total time passed since the installation, reconfiguration, or removal was initiated (0:04:56.906).

Example:

```
TASK [Add columns to the replicated table] ****************************************

Tuesday, October 31, 2023 10:29:14 +0300 (0:00:02.611) 0:04:56.906 *******
```

Component logs

By default, only errors are logged for all KUMA components. To receive detailed data in logs, configure **Debug** mode in the component settings.

The KUMA Core log is replenished to a maximum size of 5 GB or a maximum lifetime of seven days, whichever comes first. The logs of other KUMA components are appended until the file reaches 5 GB. After that, the log is archived and events start being recorded in a new log. Each log archive is stored for seven days and then deleted. A maximum of four log archives per component are stored on the server at the same time. When a fifth archive is created, the oldest archive is deleted.

Debug mode is available for the following objects:

Core	You can enable it in the KUMA web interface, in the **Settings** → **Other** → **General** → **Core settings** → **Debug** section. Storage location: `/opt/kaspersky/kuma/core/<KUMA Core service ID>/log/core` You can download Core logs in the KUMA web interface in the **Resources** → **Active services** section. To do this, select the Core service, click the menu icon (⋮) and select **Download** → **Download log**. If KUMA is installed in a high availability configuration, refer to the *Viewing Core logs in Kubernetes* section below.

Services:
 	
• Storage
• Correlators
• Collectors
• Metrics
• Agents
	To enable it, use the **Debug** toggle switch in the settings of the service.
	
	Storage location: in the service installation directory, for example `/opt/kaspersky/kuma/<collector|correlator|storage|metrics service type>/<service ID>/log/<collector|correlator|storage|metrics service type>`.
	
	You can download service logs in the KUMA web interface in the **Resources** → **Active services** section. To do this, select a service, click the menu icon (⋮) and select **Download** → **Download log**.
	
	The logs residing on Linux computers can be viewed by running the `journalctl` and `tail` commands. For example:
	
	• Storage. To return the latest logs from the storage installed on the server, run the following command:
	`journalctl -f -u kuma-storage-<storage ID>`
	• Correlators. To return the latest logs from correlators installed on the server, run the following command:
	`journalctl -f -u kuma-correlator-<correlator ID>`
	• Collectors. To return the latest logs from a specific collector installed on the server, run the following command:
	`journalctl -f -u kuma-collector-<collector ID>`
	• Metrics. To return the latest logs from a specific collector installed on the server, run the following command:
	`journalctl -f -u kuma-metrics-<metrics service ID>`
	• Agents. To return the latest logs from an agent installed on the server, run the following command:
	`tail -f /opt/kaspersky/agent/<Agent ID>/log/agent`
	The activity of Agents on Windows computers is always logged if they are assigned the logon as a service permission. Data is specified in more detail when the **Debug** check box is selected. Agent logs on Windows computers can be viewed in the file located at `%PROGRAMDATA%\Kaspersky Lab\KUMA\<agent ID>\agent.log`. Logs of Agents on Linux computers are stored in the agent installation directory.

Resources: • Connectors • Destinations • Enrichment rules	To enable it, use the **Debug** toggle switch in the settings of the service to which the resource is linked. The logs are stored on the computer hosting the installed service that uses the relevant resource. Detailed data for resources can be viewed in the log of the service linked to a resource.

Viewing Core logs in Kubernetes

When KUMA Core log files reach 100 MB, they are archived and a new log is written. No more than 5 files are stored at a time. If there are more than 5 files when a new log is created, the oldest file is deleted.

On worker nodes, you can view the logs of buckets and pods located on these nodes in the node file system, for example:

`/var/log/pods/kuma_core-deployment-<UID>/core/*.log`

To view the bucket logs:

```
k0s kubectl logs -l app=core -n kuma
```

To enable real-time log viewing, add the `-f` switch:

```
k0s kubectl logs -f -l app=core -n kuma
```

To view the logs of the previous pod that was overwritten by a new one (for example, when recovering from a critical error or after redeployment), add the `--previous` switch:

```
k0s kubectl logs -l app=core -n kuma --previous
```

To access logs from other hosts outside the cluster, you need the `k0s-kubeconfig.yml` file with access credentials, which is created during KUMA installation, and the locally installed `kubectl` cluster management utility. The `k0s-kubeconfig.yml` file is created in the `artifacts` directory in the installer directory. The cluster controller or traffic balancer specified in the `server` parameter of the `k0s-kubeconfig.yml` file must be accessible over the network.

The file path must be exported to a variable:

```
export KUBECONFIG=/<file path>/k0s-kubeconfig.yml
```

To view the logs, use the `kubectl` utility:

```
kubectl logs -l app=core -n kuma
```

Port check

All of the commands below are to be run on Linux hosts.

How to get a list of open ports and add a port on the firewall

To get a list of open ports on the firewall, run the command:

```
firewall-cmd --list-ports
```

or

```
sudo ufw status numbered
```

To add a port on the firewall, for example port 7210, run the command:

```
firewall-cmd --add-port=7210/tcp --permanent
```

or

```
sudo ufw allow 7210/tcp
```

To apply the changes made with the `firewall-cmd` commands, run the command:

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

How to check if a specific port is listening

To check if a port is listening, for example, port 5144, run the command:

```
netstat -antplu | grep 5144
```

How to check if events are received on a port

To check if events are received on a port, for example, on port 5144, run the command:

```
tcpdump -i any port 5144 -A
```

How to send a test event to a port

A test event can be sent to the port to verify that the collector is configured correctly. Below are examples of commands that you can run to send a test event to port 5144.

If you want a more complex check by sending a large number of real events, follow the instructions in the Sending test events to KUMA section.

To send an event to TCP port 5144, run the command:

```
nc 127.0.0.1 5144 <<< 'CEF:0|TESTVENDOR|TESTPRODUCT|1.1.1.1|TEST_EVENT|This is a test event|Low|message="just a test coming through"'
```

To send an event to UDP port 5144, run the command:

```
nc -u 127.0.0.1 5144 <<< 'CEF:0|TESTVENDOR|TESTPRODUCT|1.1.1.1|TEST_EVENT|This is a test event|Low|message="just a test coming through"'
```

If both types of quotation marks (' and ") are present in the raw event, the event should be written to the `test.txt` file on a single line. Then send the event to UDP port 5144 using the command:

```
cat test.txt | nc -u 127.0.0.1 5144
```

To send the event using the HTTP protocol, run the command:

```
curl -X POST -d "Your message here" http://localhost:<port>/path
```

If you want to send a multi-line event in a file using the \0 delimiter, run the command:

```
truncate -s +1 sample
curl http://<ip/host>:<port>/input --data-binary "@/root/sample"
```

Useful articles

How to configure listening on ports below 1024

Resolving the problem of insufficient disk space

Configuring the automatic deletion of old partitions

Configure the **Retention policy options** setting in the storage properties. You can limit the maximum storage size by specifying the value either in gigabytes or as a percentage of the available disk space. When the storage reaches the specified size, events are automatically transferred to cold storage disks or deleted from the ClickHouse cluster, starting with the partitions with the oldest date.

Disk space is running out, automatic deletion of data

If disk space has not completely run out and you want to automatically delete old partitions, do the following:

1. Configure the **Retention policy options** setting in the storage properties.
2. Restart the storage services.

Old partitions will be deleted in about an hour.

> If you have cold storage disks configured and you have run out of space on these, the storage service stops.

Disk space is running out, deleting data manually

If disk space has not completely run out, you can delete the oldest partitions manually.

Disk space has run out, deploying the solution on a single server

If the KUMA solution is deployed on a single server, disk space has run out and you can't log in to the KUMA web interface, do the following:

1. Stop all KUMA services using the following command:

```
systemctl stop kuma-*
```

2. Delete the collector and correlator buffers using the commands:

```
rm -rf /opt/kaspersky/kuma/collector/*/buffers/*
```

```
rm -rf /opt/kaspersky/kuma/correlator/*/buffers/
```

3. Delete the enrichment cache (if any) of the collectors and correlator using the commands:

```
rm -rf /opt/kaspersky/kuma/collector/*/cache/enrichment/*
```

```
rm -rf /opt/kaspersky/kuma/correlator/*/cache/enrichment/
```

4. Delete ClickHouse log files using the command:

```
rm -rf /opt/kaspersky/kuma/storage/*/logs/
```

5. Start ClickHouse using the command:

```
systemctl start kuma-storage*
```

6. Start the kuma-core service:

```
systemctl start kuma-core-<service ID>
```

7. Log in to the KUMA web interface and delete old partitions manually (see the instructions earlier in this article).

8. Start the remaining KUMA services:

```
sudo systemctl start kuma-<collector/correlator/metrics>-<service ID>.service
```

You can also delete KUMA service logs.

Disk space has run out, distributed deployment of the solution

If storage is deployed on separate servers and disk space has run out, do the following:

1. Stop all collectors and correlators. New events must not arrive in the storage.

   You can skip this step if the collectors and correlators are installed on a server other than the storage server. In this case, while you are following the steps, the events are saved to the buffers of the collector and correlator services.

2. Stop the kuma-storage service on the storage servers.

3. Clean up the log files using the command:

```
rm -rf /opt/kaspersky/kuma/storage/*/logs/
```

4. Clean up the buffer files using the command:

```
rm -rf /opt/kaspersky/kuma/storage/*/buffers/
```

5. Start the storage service using the command:

```
systemctl start kuma-storage-*.service
```

6. Log in to the KUMA web interface and delete old partitions manually (see the instructions earlier in this article).

Configuring notifications about disk space usage

In the **Settings** → **Other** → **Services monitoring** → **Storage** section, you can specify threshold values for a disk space. When these thresholds are reached, KUMA creates an audit event, sends a notification, and marks the corresponding service with a color indicator.

Clearing storage data completely

To completely delete storage data, run the following commands on each storage device and keeper:

```
systemctl stop kuma-storage-*.service
```

```
rm -rf /opt/kaspersky/kuma/clickhouse/data
```

```
rm -rf /opt/kaspersky/kuma/clickhouse/coordination
```

```
rm -rf /opt/kaspersky/kuma/clickhouse/logs/
```

If necessary, you can also delete temporary data:

```
rm -rf /opt/kaspersky/kuma/clickhouse/tmp/
```

```
rm -rf /opt/kaspersky/kuma/storage/*/buffers/
```

Finally, start the storage service:

```
systemctl start kuma-storage-*.service
```

Fixing the "Access denied" error when logging in to KUMA via AD FS

When you try to log in to KUMA using AD FS, the `Access denied` or `Insufficient rights` pop-up message may appear. The KUMA Core log shows the `Data source certificate has been changed` error.

This error indicates that the AD FS certificate has been changed. To fix the error and resume domain authentication, in domain controller connection settings, click the **Reset certificate** button. A new certificate will be generated automatically.

Reissuing k0s cluster certificates upon expiration

Problem

Controllers or worker nodes cannot connect; pods cannot be moved from one worker node to another.

Logs of the `k0scontroller` and `k0sworker` services contain multiple records with the following substring:

```
x509: certificate has expired or is not yet valid
```

Cause

Cluster service certificates are valid for 1 year from the time of creation. The k0s cluster used in the high-availability KUMA configuration automatically rotates all the service certificates it needs, but the rotation is performed only at startup of the `k0scontroller` service. If `k0scontroller` services on cluster controllers run without a restart for more than 1 year, service certificates become invalid.

How to fix

To fix the error, restart the `k0scontroller` services one by one as root on each controller of the cluster.

```
systemctl restart k0scontroller
```

This reissues the certificates.

To check the expiration dates of certificates on controllers, run the following commands as root:

```
find /var/lib/k0s/pki/ -type f -name "*.crt" -print|egrep -v 'ca.crt$'|xargs -L 1 -t  -i bash -c 'openssl x509  -
noout -text -in {}|grep After'
```

```
find /var/lib/k0s/pki/etcd -type f -name "*.crt" -print|egrep -v 'ca.crt$'|xargs -L 1 -t  -i bash -c 'openssl x509
-noout -text -in {}|grep After'
```

You can find the names of certificate files and their expiration dates in the output of these commands.

Resolving the DB::Exception error when updating KUMA

After updating KUMA, the storage may have a red status, and its logs may show errors.

Example error:

```
DB::Exception::Exception(std::__1::basic_string<char, std::__1::char_traits<char>,
std::__1::allocator<char>> const&, int, bool) @ 0xda0553a in
/opt/kaspersky/kuma/clickhouse/bin/clickhouse
```

To restart ClickHouse, carry out the following command on the KUMA storage server:

```
touch /opt/kaspersky/kuma/clickhouse/data/flags/force_restore_data && systemctl restart kuma-storage-<storage id>
```

Where `storage id` is the ID of the storage in which the error was detected.

Merging duplicate assets

As a result of importing asset information from different sources, the list of assets in KUMA may contain duplicates of the same assets. You can contact Technical Support to get an utility that lets you analyze the list of assets and merge duplicate assets.

REST API

You can access KUMA from third-party solutions using the API. The KUMA REST API operates over HTTP and consists of a set of request/response methods.

REST API v3 is supported.

Open REST API Help

REST API requests must be sent to the following address:

```
https://<KUMA Core FQDN>:<REST API port>/api/<API version>/<request>
```

Example

```
https://kuma.example.com:7223/api/v3
```

By default the 7223 port is used for API requests. You can change the port.

To change port used for REST API requests:

1. Log in to the server OS where the KUMA Core is installed.
2. In the file `/etc/systemd/system/multi-user.target.wants/kuma-core.service` change the following string, adding required port:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --external :7220 --internal :7210 --rest <required port number for REST API requests>
   ```

3. Restart KUMA by running the following commands in sequence:

   ```
   systemctl daemon-reload
   systemctl restart kuma-core
   ```

   New port is used for REST API.

> Make sure that the port is available and is not closed by the firewall.

Authentication header:

```
Authorization: Bearer <token>
```

Default data format: JSON

Date and time format: RFC 3339

Intensity of requests: unlimited

Creating a token

To generate a token for a user:

1. In the KUMA web interface, open **Settings** → **Users**.

   In the right part of the **Settings** section the **Users** table will be displayed.

2. Select the relevant user and click the **Generate token** button in the details area that opens on the right.

   The **New token** window opens.

3. If necessary, set the token expiration date:

   - Select the **No expiration date** check box.
   - In the **Expiration date** field, use the calendar to specify the date and time when the created token will expire.

4. Click the **Generate token** button.

   When you click this button, the user details area displays a field containing the automatically created token. When the window is closed, the token is no longer displayed. If you did not copy the token before closing the window, you will have to generate a new token.

5. Click **Save**.

The token is generated and can be used for API requests. These same steps can be taken to generate a token in your account profile.

Configuring permissions to access the API

In KUMA, you can configure which operations each user can perform. Permissions can be configured only for users created in KUMA.

To configure available operations for a user:

1. In the KUMA web interface, open **Settings** → **Users**.

   In the right part of the **Settings** section the **Users** table will be displayed.

2. Select the relevant user and click the **API access rights** button in the details area on the right.

   This opens a window containing a list of available operations. By default, all API requests are available to a user.

3. Select or clear the check box next to the relevant operation.

4. Click **Save**.

Available operations for the user are configured.

The available operations can be configured in the same way in your account profile.

Authorizing API requests

Each REST API request must include token-based authorization. The user whose token is used to make the API request must have the permissions to perform this type of request.

Each request must be accompanied by the following header:

```
Authorization: Bearer <token>
```

The following table lists possible errors.

Possible errors

HTTP code	Description	message field value	details field value
400	Invalid header	`invalid authorization header`	`Example: <example>`
403	The token does not exist or the owner user is disabled	`access denied`	

Standard error

Errors returned by KUMA have the following format:

```
type Error struct {
    Message    string      `json:"message"`
    Details    interface{} `json:"details"`
}
```

Appendices

This section provides information that complements the main document text with reference information.

KUMA settings in the inventory file

The inventory file may include the following blocks:

- `all`
- `kuma`
- `kuma_k0s`

For each host, you must specify the FQDN in the `<host name>.<domain>` format and, if necessary, an IPv4 or IPv6 address. The KUMA Core domain name and its subdomains may not start with a numeral.

Example

```
hosts:
  hostname.example.com:
    ip: 0.0.0.0
```

The 'all' block

In this block, you can specify the variables that apply to all hosts listed in the inventory file, including the implicitly specified `localhost` on which the installation is started. Variables can be overridden at the level of host groups or individual hosts.

Example of overriding variables in the inventory file

```
all:
  vars:
    ansible_connection: ssh
    deploy_to_k8s: False
    need_transfer: False
    airgap: True
    deploy_example_services: True
kuma:
  vars:
    ansible_become: true
    ansible_user: i.ivanov
    ansible_become_method: su
    ansible_ssh_private_key_file: ~/.ssh/id_rsa
  children:
    kuma_core:
      vars:
        ansible_user: p.petrov
        ansible_become_method: sudo
```

The table below shows a list of possible variables in the `vars` section and their descriptions.

List of possible variables in the vars section

Variable	Description
`ansible_connection`	Method used to connect to target computers. Possible values: • `ssh` to connect to remote hosts over SSH. If you are using a non-standard port to connect to remote hosts via SSH, specify the values for the `ansible_port` variable. • `local` to establish no connection with remote hosts.

Variable	Description

`ansible_port`	Variable for specifying a non-standard port for connecting to remote hosts via SSH. The `ansible_port` variable can be configured in the following ways:
	• If the same non-standard port is used on all hosts listed in the inventory file, specify the value of the `ansible_port` variable in the inventory file in the `all` block of the `vars` section.
	Example of a distributed.inventory.yml inventory file with the same non-standard port for all hosts
	`all:`
	`  vars:`
	`  ansible_port: 2222`
	`  deploy_to_k8s: false`
	`  need_transfer: false`
	`  generate_etc_hosts: false`
	`  deploy_example_services: false`
	`  no_firewall_actions: false`
	`kuma:`
	`  vars:`
	`  ansible_connection: ssh`
	`  ansible_user: root`
	`  children:`
	`  kuma_core:`
	`  hosts:`
	`  kuma-core-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_collector:`
	`  hosts:`
	`  kuma-collector-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_correlator:`
	`  hosts:`
	`  kuma-correlator-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_storage:`
	`  hosts:`
	`  kuma-storage-cluster1-server1.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 1`
	`  keeper: 0`
	`  kuma-storage-cluster1-server2.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 2`
	`  keeper: 0`
	`  kuma-storage-cluster1-server3.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 2`
	`  replica: 1`
	`  keeper: 0`
	`  kuma-storage-cluster1-server4.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 2`
	`  replica: 2`
	`  keeper: 0`
	`  kuma-storage-cluster1-server5.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 1`
	`  kuma-storage-cluster1-server6.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 2`
	`  kuma-storage-cluster1-server7.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 0`
	`  replica: 0`
	`  keeper: 3`
	• If you are using a non-standard port for a group of hosts, specify the value of the variable for the group of hosts in the inventory file in the `kuma` or `kuma_k0s` block in the `vars` section. For example:
	Example of a distributed.inventory.yml inventory file with the same non-standard port for a group of storage hosts
	`all:`
	`  vars:`
	`  deploy_to_k8s: false`
	`  need_transfer: false`
	`  generate_etc_hosts: false`
	`  deploy_example_services: false`
	`  no_firewall_actions: false`
	`kuma:`
	`  vars:`
	`  ansible_connection: ssh`
	`  ansible_user: root`
	`  children:`
	`  kuma_core:`
	`  hosts:`
	`  kuma-core-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_collector:`
	`  hosts:`
	`  kuma-collector-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_correlator:`
	`  hosts:`
	`  kuma-correlator-1.example.com:`
	`  ip: 0.0.0.0`
	`  kuma_storage:`
	`  vars:`
	`  ansible_port: 2222`
	`  hosts:`
	`  kuma-storage-cluster1-server1.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 1`
	`  keeper: 0`
	`  kuma-storage-cluster1-server2.example.com:`
	`  ip: 0.0.0.0`
	`  shard: 1`
	`  replica: 2`

Variable	Description

```
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

Example of a k0s.inventory.yml inventory file with the same non-standard port for all hosts in the kuma_control_plane section

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
    kuma_storage:
      hosts:
        kuma-storage-cluster1.server1.example.com
        kuma-storage-cluster1.server2.example.com
        kuma-storage-cluster1.server3.example.com
        kuma-storage-cluster1.server4.example.com
        kuma-storage-cluster1.server5.example.com
        kuma-storage-cluster1.server6.example.com
        kuma-storage-cluster1.server7.example.com
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      vars:
        ansible_port: 2222
      hosts:
        kuma_cp2.example.com:
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
        kuma-w1.example.com:
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-
default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-
default-disk=true"
```

Example of a distributed.inventory.yml inventory file for a high-availability installation with KUMA Core in a Raft cluster with the same non-standard port for all KUMA Core hosts

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
          raft_node_addr: ""
          ansible_port: 2222
    kuma_core_peers:
      vars:
        ansible_port: 2222
      hosts:
        kuma-core-2.example.com:
```

Variable	Description

```
          ip: 0.0.0.0
        kuma-core-3.example.com:
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

- If you are using a different non-standard SSH connection port for each host, specify the value of the ansible_port variable for each host in the inventory file.
  Example of a distributed.inventory.yml inventory file with a different non-standard port for each storage host

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_ssh_private_key_file: <full path to the file with the SSH key>
    ansible_user: <user from the sudo group>
    ansible_become: true
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          raft_node_addr: ""
          ip: 0.0.0.0
    kuma_metrics:
      hosts:
        kuma-metrics.example.com
          ip: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ansible_port: 2222
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ansible_port: 2223
          ip: 0.0.0.0
    kuma_storage:
      vars:
        ansible_port: 2224
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server2.example.com:
          ip: 0.0.0.0
          shard: 1
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server3.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 1
          keeper: 0
        kuma-storage-cluster1-server4.example.com:
          ip: 0.0.0.0
          shard: 2
          replica: 2
          keeper: 0
        kuma-storage-cluster1-server5.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 1
```

Variable	Description

```
        kuma-storage-cluster1-server6.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 2
        kuma-storage-cluster1-server7.example.com:
          ip: 0.0.0.0
          shard: 0
          replica: 0
          keeper: 3
```

Example of a k0s.inventory.yml inventory file with a different non-standard port for each hosts in the kuma_control_plane group

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: true
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
    metrics_disk_request: 150Gi
    core_disk_request: 100Gi
kuma:
  children:
    kuma_collector:
      hosts:
        kuma-collector.example.com:
    kuma_correlator:
      hosts:
        kuma-correlator.example.com:
    kuma_storage:
      hosts:
        kuma-storage-cluster1.server1.example.com
        kuma-storage-cluster1.server2.example.com
        kuma-storage-cluster1.server3.example.com
        kuma-storage-cluster1.server4.example.com
        kuma-storage-cluster1.server5.example.com
        kuma-storage-cluster1.server6.example.com
        kuma-storage-cluster1.server7.example.com
kuma_k0s:
  children:
    kuma_lb:
      hosts:
        kuma-lb.example.com:
          kuma_managed_lb: true
    kuma_control_plane_master:
      hosts:
        kuma_cpm.example.com:
          ansible_host: 10.0.1.10
    kuma_control_plane_master_worker:
    kuma_control_plane:
      hosts:
        kuma_cp2.example.com:
          ansible_port: 2222
          ansible_host: 10.0.1.11
        kuma_cp3.example.com:
          ansible_port: 2223
          ansible_host: 10.0.1.12
    kuma_control_plane_worker:
    kuma_worker:
      hosts:
        kuma-w1.example.com:
          ansible_host: 10.0.2.11
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-
default-disk=true"
        kuma-w2.example.com:
          ansible_host: 10.0.2.12
          extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-
default-disk=true"
```

Example of a distributed.inventory.yml inventory file for a high-availability installation with KUMA Core in a Raft cluster with a different non-standard port for each KUMA Core host

```
all:
  vars:
    deploy_to_k8s: false
    need_transfer: false
    generate_etc_hosts: false
    deploy_example_services: false
    no_firewall_actions: false
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_core:
      hosts:
        kuma-core-1.example.com:
          ip: 0.0.0.0
          raft_node_addr: ""
          ansible_port: 2222
    kuma_core_peers:
      hosts:
        kuma-core-2.example.com:
          ip: 0.0.0.0
          ansible_port: 2223
        kuma-core-3.example.com:
          ip: 0.0.0.0
          ansible_port: 2224
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
          ip: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
          ip: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-cluster1-server1.example.com:
          ip: 0.0.0.0
          shard: 1
```

Variable	Description
| | ```
    replica: 1
    keeper: 0
  kuma-storage-cluster1-server2.example.com:
    ip: 0.0.0.0
    shard: 1
    replica: 2
    keeper: 0
  kuma-storage-cluster1-server3.example.com:
    ip: 0.0.0.0
    shard: 2
    replica: 1
    keeper: 0
  kuma-storage-cluster1-server4.example.com:
    ip: 0.0.0.0
    shard: 2
    replica: 2
    keeper: 0
  kuma-storage-cluster1-server5.example.com:
    ip: 0.0.0.0
    shard: 0
    replica: 0
    keeper: 1
  kuma-storage-cluster1-server6.example.com:
    ip: 0.0.0.0
    shard: 0
    replica: 0
    keeper: 2
  kuma-storage-cluster1-server7.example.com:
    ip: 0.0.0.0
    shard: 0
    replica: 0
    keeper: 3
``` |
`ansible_user`	User name used to connect to target computers and install components. If root login is blocked on the target computers, choose a user that has the right to establish SSH connections and elevate privileges using `su` or `sudo`.
`ansible_become`	This variable specifies if you want to elevate the privileges of the user that is used to install KUMA components. Possible values: • You must specify `true` if `ansible_user` is not `root`. • `false`.
`ansible_become_method`	Method for elevating the privileges of the user that is used to install KUMA components. You must specify `su` or `sudo` if `ansible_user` is not `root`.
`ansible_ssh_private_key_file`	Path to the private key in the format `/<path>/.ssh/id_rsa`. You must specify this variable if you want to use a key file other than the default key file (`~/.ssh/id_rsa`).
`deploy_to_k8s`	This variable specifies whether you want to deploy KUMA components in a Kubernetes cluster. Possible values: • The `false` value is specified in the `single.inventory.yml` and `distributed.inventory.yml` inventory file templates. • The `true` value is specified in the `k0s.inventory.yml` inventory file template. If you do not specify this variable, it defaults to `false`.
`need_transfer`	This variable specifies whether you want to migrate KUMA Core to a new Kubernetes cluster. You need to specify this variable only if `deploy_to_k8s` is `true`. Possible values: • `false` means KUMA must be installed or updated on the Kubernetes cluster. • `true` means KUMA Core must be migrated to a new Kubernetes cluster. If you do not specify this variable, it defaults to `false`.
`no_firewall_actions`	This variable specifies whether the installer must perform the steps to configure the firewall on the hosts. Possible values: • `true` means that at startup, the installer does not perform the steps to configure the firewall on the hosts. • `false` means that at startup, the installer performs the steps to configure the firewall on the hosts. This is the value that is specified in all inventory file templates. If you do not specify this variable, it defaults to `false`.
```

Variable	Description
`generate_etc_hosts`	This variable specifies whether the computers must be registered in the DNS zone of your organization. The installer automatically adds the IP addresses of the computers from the inventory file to the `/etc/hosts` files on the computers on which KUMA components are installed. The specified IP addresses must be unique. Possible values: • `false`. • `true`. If you do not specify this variable, it defaults to `false`. When using `generate_etc_hosts: true` in the inventory file for a high-availability configuration, you must specify the balancer IP address in the `ansible_host` variable for the balancer host in the `kuma_lb` section.
`deploy_example_services`	This variable specifies whether predefined services (collector, correlator, storage) are created during the installation of KUMA. You need to specify this variable if you want to create demo services independently of the `single/distributed/k0s` inventory file. Possible values: • `false` means predefined services are not created when installing KUMA. This is the value that is specified in all inventory file templates. • `true` means predefined services are created when installing KUMA. If you do not specify this variable, it defaults to `false`.
`low_resources`	This variable specifies whether KUMA is being installed in an environment with limited computational resources. This variable is not specified in any of the inventory file templates. Possible values: • `false` means KUMA is being installed for production use. In this case, the installer checks the requirements of the worker nodes (CPU, RAM, and free disk space) in accordance with the hardware and software requirements. If the requirements are not satisfied, the installation is aborted with an error message. • `true` means that KUMA is being installed in an environment with limited computational resources. In this case, the minimum size of the KUMA Core installation directory on the host is 4 GB. All other computational resource limitations are ignored. If you do not specify this variable, it defaults to `false`.
`core_disk_request`	This variable sets the size of the KUMA Core volume for an installation in a Kubernetes cluster. If this variable is not set, the following default values are used for the KUMA Core volume size during installation: • If `low_resources=false`, the default volume size is 100Gi. • If `low_resources=true`, the default volume size is 4Gi. The 'Gi' suffix is required.
`metrics_disk_request`	This variable sets the size of the Metrics service volume for an installation in a Kubernetes cluster. If this variable is not set, the following default values are used for the Metrics server volume size during installation: • If `low_resources=false`, the default volume size is 80Gi. • If `low_resources=true`, the default volume size is 4Gi. The 'Gi' suffix is required.
`metrics_transfer_job_timeout`	This variable sets the timeout in minutes for copying metrics from a KUMA 3.4 Core volume to a new metrics volume in KUMA 4.0. The default setting is 120m. The 'm' suffix is required.
`mtu`	This variable allows you to set the maximum size of data that can be transmitted in one packet over the network medium in the Kubernetes cluster without the need for fragmentation. To solve the problem with excessive retransmission of packets or complete loss of connectivity in the encrypted link, we recommend specifying an `mtu` less than the minimum `mtu` of the existing link between the worker nodes. If no value is specified, the size of data is automatically determined based on the types of host interfaces.

Variable	Description
`backup_timeout`	This variable allows setting a maximum time in seconds allotted for creating a backup copy of the KUMA Core and separately for restoring data from a backup copy in the Kubernetes cluster. For example, if you set this variable to 2700, it means that 2700 seconds is allocated for the creation of a backup copy and 2700 seconds for restoration from a backup copy. If this setting is not specified in the 'vars' section of the inventory file, the default value is applied when automatically creating a backup copy of the KUMA Core or automatically restoring data from backup. The default value is 1800 seconds. If the automatic backup is completed before the specified time elapses, the upgrade script proceeds with the next step immediately. It makes sense to change this setting if manually creating a backup copy of the KUMA Core takes close to 30 minutes or more.

The 'kuma' block

In this block, you can specify the settings of KUMA components deployed outside of the Kubernetes cluster. The `kuma` block can contain the following sections:

- `vars` contains variables that apply to all hosts specified in the `kuma` block.
- `children` contains groups of settings for components:
  - `kuma_core` contains settings of the KUMA Core.
    - `raft_node_addr` is the address to be used for the cluster of nodes with the KUMA Core service. This address must be public and known to other nodes. After the KUMA Core is started for the first time with this address, the address cannot be changed anymore for this node. This value must be specified in the `<FQDN>:<port>` format. If this setting is not specified explicitly, `<FQDN>` defaults to the FQDN of the host on which the KUMA Core is deployed, and `<port>` defaults to 7209. The `raft_node_addr` setting must be specified together with the `raft_node_listen setting on each KUMA Core server with if DNS is configured in such a way that the server contains multiple FQDNs`. Optional setting.
    - `raft_node_listen` is the address at which the node listens for messages from its peers in the cluster. This setting must be specified in the following format `<IPv4 or IPv6 address of the KUMA Core server>:<port>`. This address can be changed. The `raft_node_listen` setting must be specified together with the raft_node_addr setting on every KUMA Core server. Optional setting.
  - `kuma_core_peers` contains settings of additional KUMA Cores. The installer prepares the servers specified in the `kuma_core_peers` section for the subsequent installation of additional KUMA Core services. You must specify an even number of servers in this section. If the `kuma_core_peers` section is missing from the inventory file or is empty, the normal installation or upgrade procedure with a single KUMA Core is performed. Only one KUMA Core service can be installed on each server in the `kuma_core_peers` group.

    Using the kuma_core_peers section for different installer use cases

Installer use case	The inventory file contains a kuma_core_peers group	The inventory file does not contain a kuma_core_peers group or the group is empty
Installation using the install.sh installer	Servers from the group are prepared for running the KUMA Core service. The kuma-core-00000000-0000-0000-0000-000000000000 service is installed on a server from the kuma_core group (displayed as core-1 in the web interface). On all servers from the kuma_core_peers group, the kuma-core-UID services are sequentially installed and started (displayed as core-<FQDN> in the web interface). These services are connected to the core-1 service. All additional services also connect to mongoDB running on the core-1 host, so the mongoDB is bound to all IP addresses of the core-1 server, and port 27017/tcp is allowed on the firewall.	A standard installation is performed with one core-1 service and one metrics service on a server from the kuma_core group.
Upgrading from version 3.4.x using the install.sh installer	Servers from the kuma_core_peersgroup are prepared for running the KUMA Core service. KUMA Core services are not installed on these servers. You can later create additional KUMA Core services in the web interface and install these on the prepared servers.	Normal upgrade is performed, the old metrics services are replaced by the new servers running on the server from the kuma_core group.
Expanding the installation using the expand.sh installer	You can create or expand a Raft cluster in an existing installation. To do this, you need to create an expand.inventory.yml inventory file, but fill in only the kuma_core_peers group. After running the expand.sh installer with the expand.inventory.yml inventory file, you need to manually create the KUMA Core services in the web interface and install them on the servers prepared by the installer. After expanding the Raft cluster, we recommend reflecting the changes in the kuma_core_peers group in the inventory file distributed.inventory.yml in case you need to upgrade KUMA.	A normal installation expansion is performed.

- `raft_node_addr` is the address to be used for the cluster of nodes with the KUMA Core service. This address must be public and known to other nodes. After the KUMA Core is started for the first time with this address, the address cannot be changed anymore for this node. This value must be specified in the `<FQDN>:<port>` format. If this setting is not specified explicitly, <FQDN> defaults to the FQDN of the host on which the KUMA Core is deployed, and `<port>` defaults to 7209. The `raft_node_addr` setting must be specified together with the `raft_node_listen setting on each KUMA Core server with if DNS is configured in such a way that the server contains multiple FQDNs`. Optional setting.

- `raft_node_listen` is the address at which the node listens for messages from its peers in the cluster. This setting must be specified in the following format `<IPv4 or IPv6 address of the KUMA Core server>:<port>`. This address can be changed. The `raft_node_listen` setting must be specified together with the raft_node_addr setting on every KUMA Core server. Optional setting.

- `kuma_metrics` contains settings of the Metrics service. You can only specify one host. When migrating the KUMA Core to a Kubernetes cluster, you must first migrate the Metrics service to the same host as the KUMA Core using the expand.sh installer and the expand.inventory.yml inventory file. When migrating the KUMA Core to a Kubernetes cluster, a check is made to see if the Metrics service is running on this host. If the Metrics service is not found, an error is returned and the migration is stopped. When you migrate the KUMA Core to a Kubernetes cluster, metrics data is migrated to the cluster.

- `kuma_collector` contains settings of KUMA collectors. You can specify multiple hosts.

- `kuma_correlator` contains settings of KUMA correlators. You can specify multiple hosts.

- `kuma_storage` contains settings of KUMA storage nodes. You can specify multiple hosts as well as shard, replica, and keeper IDs for hosts using the following settings:

  - `shard` is the shard ID.

  - `replica` is the replica ID.

  - `keeper` is the keeper ID.

The specified shard, replica, and keeper IDs are used only if you are deploying demo services as part of a fresh KUMA installation. In other cases, the shard, replica, and keeper IDs that you specified in the KUMA web interface when creating a resource set for the storage are used.

The 'kuma_k0s' block

In this block, you can specify the settings of the Kubernetes cluster that ensures high availability of KUMA. This block is specified only in an inventory file based on `k0s.inventory.yml.template`.

> For test and demo installations in environments with limited computational resources, you must also set `low_resources: true` in the `all` block. In this case, the minimum size of the KUMA Core installation directory is reduced to 4 GB and the limitations of other computational resources are ignored.

For each host in the `kuma_k0s` block, a unique FQDN and IP address must be specified in the `ansible_host` variable, except for the host in the `kuma_lb` section. For the host in the `kuma_lb` section, only the FQDN must be specified. Hosts must be unique within a group.

> For a demo installation, you may combine a controller with a worker node. Such a configuration does not provide high availability of the KUMA Core and is only intended for demonstrating the functionality or for testing the software environment.
> The minimal configuration that ensures high availability is 3 controllers, 2 worker nodes, and 1 nginx load balancer. In production, we recommend using dedicated worker nodes and controllers. If a cluster controller is under workload and the pod with the KUMA Core is hosted on the controller, if the controller goes down, access to the KUMA Core will be completely lost.

The `kuma_k0s` block can contain the following sections:

- `vars` contains variables that apply to all hosts specified in the `kuma` block.
- `children` contains settings of the Kubernetes cluster that provides high availability of KUMA.

The table below shows a list of possible variables in the `vars` section and their descriptions.

List of possible variables in the `vars` section

Variable group	Description	
`kuma_lb`	FQDN of the load balancer. You can install the nginx load balancer or a third-party TCP load balancer. If you are installing the nginx load balancer, you can set `kuma_managed_lb=true` to automatically configure the nginx load balancer when installing KUMA, open the necessary network ports on the nginx load balancer host (6443, 8132, 9443, 7209, 7210, 7220, 7222, 7223, 7226), and restart to apply the changes. If you are installing a third-party TCP load balancer, you must manually configure it before installing KUMA.	
`kuma_control_plane_master`	The host that acts as the primary controller of the cluster.	Groups for specifying the primary controller. You only need to specify a host for one group.
`kuma_control_plane_master_worker`	A host that combines the role of the primary controller and worker node in the cluster. For each cluster controller that is combined with a worker node, the following parameter must be specified in the inventory file: `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`	

Variable group	Description	
`kuma_control_plane`	Hosts that act as controllers in the cluster.	Groups for specifying secondary controllers.
`kuma_control_plane_worker`	Hosts that combine the roles of controller and worker node in the cluster. For each cluster controller that is combined with a worker node, the following parameter must be specified in the inventory file: `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`	
`kuma_worker`	Worker nodes of the cluster. For each worker node, the following parameter must be specified in the inventory file: `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`	
`kuma_metrics`	Settings of the Metrics service. You can specify only one KUMA Core host. When migrating the KUMA Core from a distributed installation to a Kubernetes cluster, you must first migrate the Metrics service to the same host as the KUMA Core using the `expand.sh` installer and the `expand.inventory.yml` inventory file. When migrating the KUMA Core to a Kubernetes cluster, a check is made to see if the Metrics service is running on this host. If the Metrics service is not found, an error is returned and the migration is stopped. When you migrate the KUMA Core to a Kubernetes cluster, metrics data is migrated to the cluster.	

`ipAutodetectionMethod`	If multiple network interfaces are being used on the worker nodes of the cluster at the same time, the `ipAutodetectionMethod` variable lets you specify a name mask of the network interface to be used for communication between the worker nodes in the cluster.
	For example, if you want to use only network interfaces named ethN (where N is the number of the network interface) for communication between worker nodes of the cluster, you can specify the variable as follows:
	`kuma_k0s:`
	`vars:`
	`ip_autodetection_method: "interface=eth.*"`
	This makes the cluster use a network interface with a name that matches the `eth.*` mask.
	If the network interface name on each worker node is the same, for example eth0, you can specify the variable without a mask:
	`kuma_k0s:`
	`vars:`
	`ip_autodetection_method: "interface=eth0"`
	For more information, please refer to the Calico Open Source documentation.	

Configuring the KUMA Core

To manage KUMA Core settings:

1. Go to the **Settings** → **Other** → **Common** section in the KUMA web interface.

2. In the **Core settings** section, specify the following settings:

   - Use the **Debug** toggle switch to enable or disable system operation logging (debug mode). The toggle switch is turned off by default.

   - If debug mode is enabled, you can use the **Dump KSC HTTP Traffic** toggle switch to enable or disable the ability to dump HTTP traffic of Kaspersky Security Center.

   - If the dumping of HTTP traffic of Kaspersky Security Center is enabled, you can use the **Periodic dumping** toggle switch to enable or disable the dumping of Kaspersky Security Center HTTP requests and responses to the event log.

     After enabling the **Enable periodic dump** check box, specify the dump settings under **Dump settings**.

- In the **Week start day** drop-down list, select the first day of the week to be used for the entire KUMA instance. The selected value is applied when selecting periods and specifying time intervals in all sections of KUMA. The default is **Monday**. Only a user with the Main administrator role can modify this setting. The selected value is saved in the KUMA Core settings.

- In the **KUMA resources localization** drop-down list, select a localization language for KUMA resources imported from the repository. The default language is English. If this setting is changed, only new KUMA resources will be imported in the selected language. If you have previously imported resources in another language, such resources will remain unchanged. To change the language of previously imported resources, you need to re-import them from the repository.

  The **KUMA resources localization** setting is independent of the KUMA language setting. You can select different localization languages in these settings. In this case, for example, the language of the texts in the resource table may differ from the localization language of the interface.

  The **KUMA resources localization** setting does not affect manually created resources.

- If necessary, click the **Reissue** button to reissue the AI service certificate and the internal CA certificate.

  > After reissuing the AI service certificate, you must manually restart all services. To apply the new AI service certificate, you must restart the KUMA Core.

3. If you do not want to use a self-signed KUMA certificate, in the **External TLS pair** section, upload a certificate and key for the TLS pair.

   By clicking the **Update certificate** button, you can update the certificate for the TLS pair.

4. Under **Core properties**, specify the following settings:

   - Select the **Compacting SQLite** check box and specify the amount of disk space in GB. This allows you to reduce the size of the database for more efficient use of disk space.

     By default, the check box is selected, and the disk space is set to 10,000 GB.

   - In the **Activation tag** field, specify an applicable tag.

   - In the **Alert retention period, days** field, specify the retention period for alerts in days. You can specify any value greater than 0.

     The default retention period is 365 days.

   - In the **Asset bulk merge size** field, specify the number of assets in one group (batch) into which the total set of assets is split before the start of the merge. Each group of assets is sequentially processed by the solution, which means assets are merged, verified and saved. If a value of 10 is specified, then 100 assets are split into 10 groups of 10 assets, and the groups are processed one by one. Specifying a smaller value yields smaller groups, which accelerates merging because the solution processes less data per step.

     You can specify any value greater than 0. The default setting is 10.

   - In the **Maximum number of services to be started simultaneously** field, specify the number of services that KUMA can start simultaneously.

     The default setting is 10.

     > Too many services running at the same time can slow down the processing of KUMA data.

- In the **Correlation rule exclusions TTL, hours** field, specify the lifetime in hours for correlation rule exclusions. You can specify a value from 1 to 8760 (24*365) inclusive.

  The default setting is 72.

- In the **Disk buffer size of service destination of Core (for sending events), MB** field, specify the size of the disk buffer on the Core that is allocated for each service. This buffer is used when internal events cannot be sent to correlators. You can set any buffer size greater than 0.

  The default setting is 1024 MB.

- In the **Timeout of sending events via service destination of Core, seconds** field, specify the timeout for establishing the connection to the service when sending events. You can specify any timeout longer than 0 seconds.

  The default setting is 15 seconds.

- In the **The hour of the day when Core is authorized to perform self-service tasks** field, specify the time (in UTC) when the Core can perform self-service operations. The Core performs such operations on a daily basis. You can specify a value from 0 to 23, inclusive.

  > We recommend performing self-service operations for the KUMA Core during nighttime, when users are not using the functionality of the Core.

  The default setting is 1 (UTC time).

- If necessary, in the **Max stored file size, MB** field, specify the maximum size of the compressed data of the downloaded GeoIP database and repository packages.

  The default maximum value is 300 MB.

- In the **Resource history retention period, days** field, specify the retention period for the resource changes history in days. You can set any value greater than or equal to 0.

  The default setting is 12 days.

- In the **Cluster request timeout from the UI, seconds** field, specify how long the KUMA web client must wait for a response after requesting the list of storages. You can set any value greater than 0.

  The default setting is 30 seconds.

- In the **Storage nodes health check timeout, seconds** field, specify the time to wait for a response after requesting an availability check of certain storage nodes. You can set any value greater than 0.

  The default setting is 30 seconds.

- If necessary, in the **KUMA UI balancer hostname and port** field, specify the host name and port of the KUMA user interface balancer.

  Given the distributed nature of the KUMA Core, multiple Core nodes can be configured to work as a cluster. You can configure the connection to the cluster through the balancer.

  > You can specify only one balancer URL.

The balancer URL must be specified in the `hostname:port` format, where

- `hostname` is the hostname of the balancer.
- `port` is the port of the balancer.

Other balancer URL formats are not allowed.

5. Click **Save**.

Commands for components manual starting and installing

This section contains the parameters of KUMA's executable file /opt/kaspersky/kuma/kuma that can be used to manually start or install KUMA services. This may be useful for when you need to see output in the server operating system console.

Commands parameters

Commands	Description
`tools`	Start KUMA administration tools.
`collector`	Install, start, or remove a collector service.
`core`	Install, start, or uninstall a Core service.
`correlator`	Install, start, or remove a correlator service.
`agent`	Install, start, or remove an agent service.
`help`	Get information about available commands and parameters.
`license`	Get information about license.
`storage`	Start or install a Storage.
`version`	Get information about the version of the solution.

Flags:

`-h`, `--h` are used to get help about any kuma command. For example, `kuma <component> --help`.

Examples:

- `kuma version` is used to get version of the KUMA installer.
- `kuma core -h` is used to get help about `core` command of KUMA installer.
- `kuma collector --core <address of the server where the collector should obtain its settings> --id <ID of the installed service> --api.port <port>` is used to start collector service installation.

Ports used by KUMA during installation

For the application to run correctly, you need to ensure that the KUMA components are able to interact with other components and applications over the network using the protocols and ports specified during the installation of the KUMA components.

Before installing KUMA, make sure that the following ports are free on the host from the `kuma_metrics` section in the inventory file, on which host you want to install the Metrics service:

- 7227
- 7228
- 8001

The table below lists the default ports. The installer automatically opens the ports during KUMA installation

Network ports used for the interaction of KUMA components

Protocol	Port	Direction	Purpose of the connection
HTTPS	7222	From the KUMA client to the KUMA Core server.	Reverse proxy to the CyberTrace system.
HTTPS	8123	Local requests from the storage service to the local node of the ClickHouse cluster.	Writing and getting normalized events in the ClickHouse cluster.
HTTPS	9009	Between replicas of the ClickHouse cluster.	Internal data communication between replicas of the ClickHouse cluster.
TCP	2181	From ClickHouse cluster nodes to the ClickHouse keeper replication coordination service.	Getting and writing replication metadata by replicas of ClickHouse servers.
TCP	2182	From one ClickHouse keeper replication coordination service to another.	Internal communication between replication coordination services to reach a quorum.
TCP	7210	From all KUMA components to the KUMA Core server.	Getting the KUMA configuration from the KUMA Core server, as well as recording the metrics of the KUMA agent.
TCP	7220	• From the KUMA client to the server with the KUMA Core component. • From storage hosts to the KUMA Core server during installation or upgrade.	• User access to the KUMA web interface. • Interaction between the storage hosts and the KUMA Core during installation or upgrade. You can close this port after completing the installation or upgrade.
TCP	7221 and other ports used for service installation as the --api.port <port> parameter value	From KUMA Core to KUMA services.	Administration of services from the KUMA web interface.
TCP	7223	To the KUMA Core server.	Default port for API requests.
TCP	8001	From the Metrics service to the ClickHouse server.	Getting ClickHouse server operation metrics.
TCP	9000	• Outgoing and incoming connections between servers of the ClickHouse cluster. • From the local client.sh client to the local cluster node.	Port of the ClickHouse native protocol (also called *ClickHouse TCP*). Used by ClickHouse applications and processes, such as clickhouse-server, clickhouse-client, and native ClickHouse tools Used for inter-server communication for distributed queries. Also used for writing and getting data in the ClickHouse cluster.

Ports used by predefined OOTB resources

The installer automatically opens the ports during KUMA installation.

Ports used by predefined OOTB resources:

- 7230/tcp
- 7231/tcp
- 7232/tcp
- 7233/tcp
- 7234/tcp
- 7235/tcp
- 5140/tcp
- 5140/udp
- 5141/tcp
- 5144/udp

KUMA Core traffic in a high availability configuration

The table below lists the initiator (source) of the connection and the destination. The port number on the initiator can be dynamic. Return traffic within the established connection must not be blocked.

KUMA Core traffic in a high availability configuration

Source	Destination	Destination port	Type
External KUMA services	Load balancer	7209	TCP
External KUMA services	Load balancer	7210	TCP
External KUMA services	Load balancer	7220	TCP
External KUMA services	Load balancer	7222	TCP
External KUMA services	Load balancer	7223	TCP
Worker node	Load balancer	6443	TCP
Worker node	Load balancer	8132	TCP
Control node	Load balancer	6443	TCP
Control node	Load balancer	8132	TCP
Control node	Load balancer	9443	TCP
Worker node	External KUMA services	Depending on the settings specified when creating the service.	TCP
Load balancer	Worker node	7209	TCP
Load balancer	Worker node	7210	TCP

Source	Destination	Destination port	Type
Load balancer	Worker node	7220	TCP
Load balancer	Worker node	7222	TCP
Load balancer	Worker node	7223	TCP
External KUMA services	Worker node	7209	TCP
External KUMA services	Worker node	7210	TCP
External KUMA services	Worker node	7220	TCP
External KUMA services	Worker node	7222	TCP
External KUMA services	Worker node	7223	TCP
Worker node	Worker node	179	TCP
Worker node	Worker node	9500	TCP
Worker node	Worker node	10250	TCP
Worker node	Worker node	51820	UDP
Worker node	Worker node	51821	UDP
Control node	Worker node	10250	TCP
Load balancer	Control node	6443	TCP
Load balancer	Control node	8132	TCP
Load balancer	Control node	9443	TCP
Worker node	Control node	6443	TCP
Worker node	Control node	8132	TCP
Worker node	Control node	10250	TCP
Control node	Control node	2380	TCP
Control node	Control node	6443	TCP
Control node	Control node	9443	TCP
Control node	Control node	10250	TCP
Cluster management console (CLI)	Load balancer	6443	TCP
Cluster management console (CLI)	Control node	6443	TCP

Network settings for interaction with external services

KUMA uses the following network settings for communication with external services.

Network settings

Network settings	Address	Description
Port: 443 Protocol: HTTPS	https://activate.activation-v2.kaspersky.com https://refresh-bkg.activation-v2.kaspersky.com https://simulate.activation-v2.kaspersky.com https://simulate-bkg.activation-v2.kaspersky.com https://activation-v2.kaspersky.com/corporate/getactivationcodeinfo Regional servers (region RU): • https://ru.activate.activation-v2.kaspersky.com • https://ru.refresh-bkg.activation-v2.kaspersky.com • https://ru.simulate.activation-v2.kaspersky.com • https://simulate-bkg.activation-v2.kaspersky.com • https://ru.activation-v2.kaspersky.com/corporate/getactivationcodeinfo	Activating the solution.

Network settings	Address	Description
Port: 443 Protocol: HTTPS	https://llm-gateway.ksn.kaspersky-labs.com	Using the KIRA service.
Port: 443 Protocol: HTTPS	https://ds.kaspersky.com https://dc1-file.ksn.kaspersky-labs.com	Using the DLL Hijacking detection feature.

Normalized event data model

This section presents the KUMA normalized event data model. All events that are processed by KUMA Correlator to detect alerts must be compliant to this model. The maximum size of an event that can be processed by the KUMA collector is 4 MB.

Events that are not compliant to this data model must be converted to this format (or normalized) using Collectors.

Normalized event data model

Field name	Data type	Field size	Description
The name of a field reflects its purpose. The fields can be modified.			
`ApplicationProtocol`	String	31 characters	Name of the application layer protocol. For example, HTTPS, SSH, Telnet.
`BytesIn`	Number	From -9223372036854775808 to 9223372036854775807	Number of bytes received.
`BytesOut`	Number	From -9223372036854775808 to 9223372036854775807	Number of bytes sent.
`DestinationAddress`	String	45 characters	IPv4 or IPv6 address of the asset that the action will be performed on. For example, 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
`DestinationCity`	String	1,023 characters	City corresponding to the IP address from the DestinationAddress field.
`DestinationCountry`	String	1023 characters	Country corresponding to the IP address from the DestinationAddress field.
`DestinationDnsDomain`	String	255 characters	The DNS portion of the fully qualified domain name of the destination.
`DestinationHostName`	String	1023 characters	Host name of the destination. FQDN of the destination, if available.
`DestinationLatitude`	Floating point number	+/- 1.7E-308 to 1.7E+308	Longitude corresponding to the IP address from the DestinationAddress field.
`DestinationLongitude`	Floating point number	+/- 1.7E-308 to 1.7E+308	Latitude corresponding to the IP address from the DestinationAddress field.
`DestinationMacAddress`	String	17 characters	MAC address of the destination. For example, aa:bb:cc:dd:ee:00
`DestinationNtDomain`	String	255 characters	Windows Domain Name of the destination.
`DestinationPort`	Number	From -9223372036854775808 to 9223372036854775807	Port number of the destination.
`DestinationProcessID`	Number	From -9223372036854775808 to 9223372036854775807	System process ID registered on the destination.

DestinationProcessName	String	1023 characters	Name of the system process registered on the destination. For example, sshd, telnet.
DestinationRegion	String	1023 characters	Region corresponding to the IP address from the DestinationAddress field.
DestinationServiceName	String	1023 characters	Name of the service on the destination side. For example, sshd.
DestinationTranslatedAddress	String	45 characters	Translated IPv4 or IPv6 address of the destination. For example, 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DestinationTranslatedPort	Number	From -9223372036854775808 to 9223372036854775807	Port number at the destination after translation.
DestinationUserID	String	1023 characters	User ID of the destination.
DestinationUserName	String	1023 characters	User name of the destination.
DestinationUserPrivileges	String	1023 characters	Names of roles that identify user privileges at the destination. For example, "User", "Guest", or "Administrator".
DeviceAction	String	63 characters	Action that was taken by the event source. For example, blocked, detected.
DeviceAddress	String	45 characters	IPv4 or IPv6 address of the device from which the event was received. For example, 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceCity	String	1023 characters	City corresponding to the IP address from the DeviceAddress field.
DeviceCountry	String	1023 characters	Country corresponding to the IP address from the DeviceAddress field.
DeviceDnsDomain	String	255 characters	DNS part of the fully qualified domain name of the device from which the event was received.
DeviceEventClassID	String	1023 characters	Event type ID assigned by the event source.
DeviceExternalID	String	255 characters	ID of the device or application assigned by the event source. If you want the DeviceExternalID field to be displayed as a link in the event properties, configure a template in the enrichment rule or in the correlation rule.
DeviceFacility	String	1023 characters	Value of the facility parameter set by the event source.
DeviceHostName	String	100 characters	Name of the device from which the event was received. FQDN of the device, if available.
DeviceInboundinterface	String	128 characters	Name of the incoming connection interface.
DeviceLatitude	Floating point number	+/- 1.7E-308 to 1.7E+308	Longitude corresponding to the IP address from the DeviceAddress field.
DeviceLongitude	Floating point number	+/- 1.7E-308 to 1.7E+308	Latitude corresponding to the IP address from the DeviceAddress field
DeviceMacAddress	String	17 characters	MAC address of the asset from which the event was received. For example, aa:bb:cc:dd:ee:00
DeviceNtDomain	String	255 characters	Windows Domain Name of the device.
DeviceOutboundinterface	String	128 characters	Name of the outgoing connection interface.
DevicePayloadID	String	128 characters	The payload's unique ID that is associated with the raw event.
DeviceProcessID	Number	From -9223372036854775808 to 9223372036854775807	ID of the system process on the device that generated the event.
DeviceProcessName	String	1023 characters	Name of the process.

DeviceProduct	String	63 characters	Name of the application that generated the event. The DeviceVendor, DeviceProduct, and DeviceVersion all uniquely identify the log source.
DeviceReceiptTime	Number	From -9223372036854775808 to 9223372036854775807	Time when the device received the event.
DeviceRegion	String	1023 characters	Region corresponding to the IP address from the DeviceAddress field.
DeviceTimeZone	String	255 characters	Time zone of the device on which the event was generated.
DeviceTranslatedAddress	String	45 characters	Re-translated IPv4 or IPv6 address of the device from which the event was received. For example, 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceVendor	String	63 characters	Vendor name of the event source. The DeviceVendor, DeviceProduct, and DeviceVersion all uniquely identify the log source.
DeviceVersion	String	31 characters	Application version of the event source. The DeviceVendor, DeviceProduct, and DeviceVersion all uniquely identify the log source.
EndTime	Number	From -9223372036854775808 to 9223372036854775807	Date and time (timestamp) when the event ended.
EventOutcome	String	63 characters	Result of the operation. For example, success, failure.
ExternalID	String	40 characters	Field in which the ID can be saved.
FileCreateTime	Number	From -9223372036854775808 to 9223372036854775807	File creation time.
FileHash	String	255 characters	Hash of the file.
FileID	String	1023 characters	ID of the file.
FileModificationTime	Number	From -9223372036854775808 to 9223372036854775807	Time when the file was last modified.
FileName	String	1023 characters	Filename without specifying the file path.
FilePath	String	1023 characters	File path, including the file name.
FilePermission	String	1023 characters	List of file permissions.
FileSize	Number	From -9223372036854775808 to 9223372036854775807	File size.
FileType	String	1023 characters	File type.
Message	String	1023 characters	Brief description of the event.
Name	String	512 characters	Name of the event.
OldFileCreateTime	Number	From -9223372036854775808 to 9223372036854775807	Time when the OLD file was created from the event. The time is specified in UTC0. In the KUMA web interface, the value is displayed based in the timezone of the user's browser.
OldFileHash	String	255 characters	Hash of the OLD file.
OldFileID	String	1023 characters	ID of the OLD file.
OldFileModificationTime	Number	From -9223372036854775808 to 9223372036854775807	Time when the OLD file was last modified.
OldFileName	String	1023 characters	Name of the OLD file (without the file path).
OldFilePath	String	1023 characters	Path to the OLD file, including the file name.
OldFilePermission	String	1023 characters	List of permissions of the OLD file.

OldFileSize	Number	From -9223372036854775808 to 9223372036854775807	Size of the OLD file.
OldFileType	String	1023 characters	Type of the OLD file.
Reason	String	1023 characters	Information about the reason for the event.
RequestClientApplication	String	1023 characters	Value of the "user-agent" parameter of the http request.
RequestContext	String	2,048 characters	Description of the http request context.
RequestCookies	String	1023 characters	Cookies associated with the http request.
RequestMethod	String	1023 characters	Method used when making the http request.
RequestUrl	String	1023 characters	Requested URL.
Severity	String	1023 characters	Priority. This can be the Severity field or the Level field of the raw event.
SourceAddress	String	45 characters	IPv4 or IPv6 address of the source. Example format: 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
SourceCity	String	1023 characters	City corresponding to the IP address from the SourceAddress field.
SourceCountry	String	1023 characters	Country corresponding to the IP address from the SourceAddress field.
SourceDnsDomain	String	255 characters	The DNS portion of the fully qualified domain name of the source.
SourceHostName	String	1023 characters	Windows Domain Name of the event source device.
SourceLatitude	Floating point number	+/- 1.7E-308 to 1.7E+308	Longitude corresponding to the IP address from the SourceAddress field.
SourceLongitude	Floating point number	+/- 1.7E-308 to 1.7E+308	Latitude corresponding to the IP address from the SourceAddress field.
SourceMacAddress	String	17 characters	MAC address of the source. Format example: aa:bb:cc:dd:ee:00
SourceNtDomain	String	255 characters	Windows Domain Name of the source.
SourcePort	Number	From -9223372036854775808 to 9223372036854775807	Source port number.
SourceProcessID	Number	From -9223372036854775808 to 9223372036854775807	System process ID.
SourceProcessName	String	1023 characters	Name of the system process at the source. For example, sshd, telnet.
SourceRegion	String	1023 characters	Region corresponding to the IP address from the SourceAddress field.
SourceServiceName	String	1023 characters	Name of the service on the source side. For example, sshd.
SourceTranslatedAddress	String	45 characters	Translated IPv4 or IPv6 address of the source. Example format: 0.0.0.0 or xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
SourceTranslatedPort	Number	From -9223372036854775808 to 9223372036854775807	Port number of the source after translation.
SourceUserID	String	1023 characters	User ID of the source.
SourceUserName	String	1023 characters	User name of the source.
SourceUserPrivileges	String	1023 characters	Names of roles that identify user privileges of the source. For example, "User", "Guest", or "Administrator".
StartTime	Number	From -9223372036854775808 to 9223372036854775807	Date and time (timestamp) when the activity associated with the event began.

`Tactic`	String	128 characters	Name of the tactic from the MITRE ATT&CK matrix.
`Technique`	String	128 characters	Name of the technique from the MITRE ATT&CK matrix.
`TransportProtocol`	String	31 characters	Name of the OSI Transport layer protocol (for example, TCP, UDP).
`Type`	Number	From -9223372036854775808 to 9223372036854775807	Event type: 1 - basic, 2 - aggregated, 3 - correlation, 4 - audit, 5 - monitoring.
Fields the purpose of which can be defined by the user. The fields can be modified.			
`DeviceCustomDate1`	Number, timestamp	From -9223372036854775808 to 9223372036854775807	Field for mapping a date and time value (timestamp). The time is specified in UTC0. In the KUMA web interface, the value is displayed based in the timezone of the user's browser.
`DeviceCustomDate1Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomDate1 field.
`DeviceCustomDate2`	Number, timestamp	From -9223372036854775808 to 9223372036854775807	Field for mapping a date and time value (timestamp). The time is specified in UTC0. In the KUMA web interface, the value is displayed based in the timezone of the user's browser.
`DeviceCustomDate2Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomDate2 field.
`DeviceCustomFloatingPoint1`	Floating point number	+/- 1.7E-308 to 1.7E+308	Field for mapping floating point numbers.
`DeviceCustomFloatingPoint1Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomFloatingPoint1 field.
`DeviceCustomFloatingPoint2`	Floating point number	+/- 1.7E-308 to 1.7E+308	Field for mapping floating point numbers.
`DeviceCustomFloatingPoint2Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomFloatingPoint2 field.
`DeviceCustomFloatingPoint3`	Floating point number	+/- 1.7E-308 to 1.7E+308	Field for mapping floating point numbers.
`DeviceCustomFloatingPoint3Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomFloatingPoint3 field.
`DeviceCustomFloatingPoint4`	Floating point number	+/- 1.7E-308 to 1.7E+308	Field for mapping floating point numbers.
`DeviceCustomFloatingPoint4Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomFloatingPoint4 field.
`DeviceCustomIPv6Address1`	String	45 characters	Field for mapping an IPv6 address value. Format example: y:y:y:y:y:y:y:y
`DeviceCustomIPv6Address1Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomIPv6Address1 field.
`DeviceCustomIPv6Address2`	String	45 characters	Field for mapping an IPv6 address value. Format example: y:y:y:y:y:y:y:y
`DeviceCustomIPv6Address2Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomIPv6Address2 field.
`DeviceCustomIPv6Address3`	String	45 characters	Field for mapping an IPv6 address value. Format example: y:y:y:y:y:y:y:y
`DeviceCustomIPv6Address3Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomIPv6Address3 field.
`DeviceCustomIPv6Address4`	String	45 characters	Field for mapping an IPv6 address value. For example, y:y:y:y:y:y:y:y
`DeviceCustomIPv6Address4Label`	String	1023 characters	Field for describing the purpose of the DeviceCustomIPv6Address4 field.
`DeviceCustomNumber1`	Number	From -9223372036854775808 to 9223372036854775807	Field for mapping an integer value.

DeviceCustomNumber1Label	String	1023 characters	Field for describing the purpose of the DeviceCustomNumber1 field.
DeviceCustomNumber2	Number	From -9223372036854775808 to 9223372036854775807	Field for mapping an integer value.
DeviceCustomNumber2Label	String	1023 characters	Field for describing the purpose of the DeviceCustomNumber2 field.
DeviceCustomNumber3	Number	From -9223372036854775808 to 9223372036854775807	Field for mapping an integer value.
DeviceCustomNumber3Label	String	1023 characters	Field for describing the purpose of the DeviceCustomNumber3 field.
DeviceCustomString1	String	4,000 characters	Field for mapping a string value.
DeviceCustomString1Label	String	1,023 characters	Field for describing the purpose of the DeviceCustomString1 field.
DeviceCustomString2	String	4,000 characters	Field for mapping a string value.
DeviceCustomString2Label	String	1023 characters	Field for describing the purpose of the DeviceCustomString2 field.
DeviceCustomString3	String	4,000 characters	Field for mapping a string value.
DeviceCustomString3Label	String	1023 characters	Field for describing the purpose of the DeviceCustomString3 field.
DeviceCustomString4	String	4,000 characters	Field for mapping a string value.
DeviceCustomString4Label	String	1023 characters	Field for describing the purpose of the DeviceCustomString4 field.
DeviceCustomString5	String	4,000 characters	Field for mapping a string value.
DeviceCustomString5Label	String	1023 characters	Field for describing the purpose of the DeviceCustomString5 field.
DeviceCustomString6	String	4,000 characters	Field for mapping a string value.
DeviceCustomString6Label	String	1023 characters	Field for describing the purpose of the DeviceCustomString6 field.
DeviceDirection	Number	From -9223372036854775808 to 9223372036854775807	Field for describing the direction of connection for an event. "0" - incoming connection, "1" - outgoing connection.
DeviceEventCategory	String	1023 characters	Event category assigned by the device that sent the event to SIEM.
FlexDate1	Number, timestamp	From -9223372036854775808 to 9223372036854775807	Field for mapping a date and time value (timestamp). The time is specified in UTC0. In the KUMA web interface, the value is displayed based in the timezone of the user's browser.
FlexDate1Label	String	128 characters	Field for describing the purpose of the FlexDate1Label field.
FlexNumber1	Number	From -9223372036854775808 to 9223372036854775807	Field for mapping an integer value.
FlexNumber1Label	String	128 characters	Field for describing the purpose of the FlexNumber1Label field.
FlexNumber2	Number	From -9223372036854775808 to 9223372036854775807	Field for mapping an integer value.
FlexNumber2Label	String	128 characters	Field for describing the purpose of the FlexNumber2Label field.
FlexString1	String	1023 characters	Field for mapping a string value.
FlexString1Label	String	128 characters	Field for describing the purpose of the FlexString1Label field.

FlexString2	String	1023 characters	Field for mapping a string value.
FlexString2Label	String	128 characters	Field for describing the purpose of the FlexString2Label field.
Service fields. Cannot be edited.			
AffectedAssets	Nested [Affected] structure	-	Nested structure from which you can query alert-related assets and user accounts, and find out the number of times they appear in alert events.
AggregationRuleID	String	-	Aggregation rule ID.
AggregationRuleName	String	-	The name of the aggregation rule that processed the event.
BaseEventCount	Number	-	For an aggregated base event, this is the number of base events that were processed by the aggregation rule. For a correlation event, this is the number of base events that were processed by the correlation rule that generated the correlation event.
BaseEvents	Nested [Event] list	-	Nested structure containing a list of base events. This field can be filled in for correlation events.
Code	String	-	In a base event, this is the code of a process, function or operation return from the source.
CorrelationRuleID	String	-	ID of the correlation rule.
CorrelationRuleName	String	-	Name of the correlation rule that triggered the creation of the correlation event. Filled only for correlation events.
DestinationAccountID	String	-	This field stores the user ID.
DestinationAssetID	String	-	This field stores the asset ID of the destination.
DeviceAssetID	String	-	This field stores the ID of the asset that sent the event to SIEM.
Extra	Nested [string:string] dictionary	-	During normalization of a raw event, this field can be used to place those fields that have not been mapped to KUMA event fields. This field can be filled in only for base events. The maximum size of the field is 4 MB.
GroupedBy	String	-	List of names of the fields that were used for grouping in the correlation rule. It is filled in only for the correlation event.
ID	String	-	Unique event ID of UUID type. For a base event that is generated on the collector, the ID is generated by the collector. The correlator generates the ID of a correlation event. The ID never changes its value.
Raw	String	-	Non-normalized text of the original raw event. Maximum field size is 16,384 bytes.
ReplayID	String	-	ID of the retroscan that generated the event.
ServiceID	String	-	ID of the service instance: correlator, collector, storage.
ServiceName	String	-	Name of the microservice instance that the KUMA administrator assigns when creating the microservice.
SourceAccountID	String	-	This field stores the user ID.
SourceAssetID	String	-	This field stores the asset ID of the event source.
SpaceID	String	-	ID of the space.
TenantID	String	-	This field stores the ID of the tenant.

`TI`	Nested [string:string] dictionary	-	Field that contains categories in a dictionary format received from an external Threat Intelligence source based on indicators from an event.
`Timestamp`	Number	-	Timestamp of the base event created in the collector. Creation time of the correlation event created by the collector. The time is specified in UTC0. In the KUMA web interface, the value is displayed based in the timezone of the user's browser.

Nested `Affected` structure

Field	Data type	Description
`Assets`	Nested `[AffectedRecord]` list	List and number of assets associated with the alert.
`Accounts`	Nested `[AffectedRecord]` list	List and number of user accounts associated with the alert.

Nested `AffectedRecord` structure

Field	Data type	Description
`Value`	String	ID of the asset or user account.
`Count`	Number	How many times an asset or user account appears in alert-related events.

Fields generated by KUMA

KUMA generates the following fields that cannot be modified: BranchID, BranchName, DestinationAccountName, DestinationAssetName, DeviceAssetName, SourceAccountName, SourceAssetName, TenantID (the field displays the name of the tenant, an enriched value, while the tenant ID is used for searching the database).

Configuring the data model of a normalized event from KATA EDR

When investigating incidents, it can be useful to build a chain of processes. For this purpose, it is important that certain fields of the normalized event contain KATA/EDR process IDs. After correctly configuring normalization, you can build a process chain for events coming from KATA/EDR using an SQL query.

Example of building a process chain using an SQL query

Example of an SQL query for selecting events containing a process chain

```
SELECT
```

```
    b.DeviceHostName AS HostName,
    b.SourceAccountID AS AccountID,
    b.SourceUserName AS UserName,
    a.DeviceCustomString3 AS GrandParentProcessID,
    a.SourceProcessName AS GrandParentProcessName,
    a.DeviceCustomString5 AS ParentProcessID,
    a.DestinationProcessName AS ParentProcessName,
    b.DeviceCustomString5 AS ProcessID,
    b.DestinationProcessName AS ProcessName,
    concat(a.SourceProcessName, ' -> ', a.DestinationProcessName, ' -> ',
b.DestinationProcessName) AS ProcessTree
FROM `events` AS a
INNER JOIN
    (
        SELECT *
        FROM `events`
        WHERE DeviceEventClassID='4688'
    ) AS b
ON a.DeviceCustomString5 = b.DeviceCustomString3
WHERE DeviceEventClassID='4688'
```

Result

As a result of the query execution, events that meet the query conditions are returned in the **Events** section. In the event card, the `ProcessTree` field lists the process chain: process A → process B → ... → process N.

For example:

```
C:\Windows\System32\svchost.exe -> C:\Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.17763.164_none_7e114a3d4d0589d4\TIWorker.exe ->
C:\Windows\System32\conhost.exe
```

To build a process chain, you need to configure the copying of data from the fields of the raw events to the fields of the normalized event in KUMA normalizers as follows:

1. For any KATA/EDR events, you must configure normalization with copying of the following fields:

   - The `EventType` field of the KATA/EDR event must be copied to the `DeviceEventCategory` field of the normalized KUMA event.

   - The `HostName` field of the KATA/EDR event must be copied to the `DeviceHostName` field of the normalized KUMA event.

2. For any event where `DeviceProduct = 'KATA'`, normalization must be configured in accordance with the table below.

Normalization of event fields from KATA/EDR

KATA/EDR event field	Normalized event field
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance
FilePath	FilePath

KATA/EDR event field	Normalized event field
FileName	FileName
Md5	FileHash
FileSize	FileSize

3. For events listed in the table below, additional normalization with field copying must be configured in accordance with the table.

Additional normalization with copying of event fields from KATA/EDR

Event	Raw event field	Normalized event field
Process	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
AppLock	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Module	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Driver	HostName	DeviceHostName
	FileName	FileName
	ProductName	DeviceCustomString5,
		ProductName
	ProductVendor	DeviceCustomString6
		ProductVendor
Connection	UniquePid	FlexString2
	HostName	DeviceHostName
	URI	RequestURL
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	HostName	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort

Event	Raw event field	Normalized event field
Registry	UniquePid	FlexString2
	HostName	DeviceHostName
	ValueName	DeviceCustomString5
		New Value Name
	KeyName	DeviceCustomString4
		New Key Name
	PreviousKeyName	FlexString2
		Old Key Name
	ValueData	DeviceCustomString6
		New Value Data
	PreviousValueData	FlexString1
		Old Value Data
	ValueType	FlexNumber1
		Value Type
	PreviousValueType	FlexNumber2
		Previous Value Type
SystemEventLog	UniquePid	FlexString2
	HostName	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID
ThreatDetect	UniquePid	FlexString2
	HostName	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		Is Silent
	RecordId	DeviceCustomString5
		Record ID
	DatabaseTimestamp	DeviceCustomDate2
		Database Timestamp
ThreatDetectProcessingResult	UniquePid	FlexString2
	HostName	DeviceHostName
	ThreatStatus	DeviceCustomString5
		Threat Status

Event	Raw event field	Normalized event field
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize
	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	HostName	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		Command Line
AMSI SCAN	UniquePid	FlexString2
	HostName	DeviceHostName
	ObjectContent	DeviceCustomString5
		Object Content

Alert data model

This section describes the KUMA alert data model. Alerts are created by correlators whenever information security threats are detected using correlation rules. Alerts must be investigated to eliminate these threats.

Alert field	Data type	Description
`ID`	String	Unique ID of the alert.
`TenantID`	String	ID of the tenant that owns the alert. The value is inherited from the correlator that generated the alert.
`TenantName`	String	Tenant name.
`CorrelationRuleID`	String	ID of the rule used as the basis for generating the alert.
`CorrelationRuleName`	String	Name of the correlation rule used as the basis for generating the alert.
`Status`	String	Alert status. Possible values: • `New`—new alert. • `Assigned`—the alert is assigned to a user. • `Closed`—the alert was closed. • `Exported to IRP`—the alert was exported to the IRP system for further investigation. • `Escalated`—an incident was generated based on this alert.
`Priority`	Number	Alert severity. Possible values: • 1–4 — Low. • 5–8 — Medium. • 9–12 — High. • 13–16 — Critical.
`ManualPriority`	`TRUE/FALSE` string	Parameter showing how the alert severity level was determined. Possible values: • `true`—defined by the user. • `false` (default value)—calculated automatically.
`FirstSeen`	Number	Time when the first correlation event was created from the alert.
`LastSeen`	Number	Time when the last correlation event was created from the alert.
`UpdatedAt`	Number	Date of the last modification to the alert parameters.

`UserID`	String	ID of the KUMA user assigned to examine the alert.
`UserName`	String	Name of the KUMA user assigned to examine the alert.
`GroupedBy`	Nested list of strings	List of event fields used to group events in the correlation rule.
`ClosingReason`	String	Reason for closing the alert. Possible values: • `Incorrect Correlation Rule`—the alert was a false positive and the received events do not indicate a real security threat. The correlation rule may need to be updated. • `Incorrect Data`—the alert was a false positive and the received events do not indicate a real security threat. • `Responded`—the appropriate measures were taken to eliminate the security threat.
`MaxAssetsWeightStr`	String	Maximum severity of the asset categories associated with the alert.
`MaxAssetCategoryImportance`	String	This field contains the value of the `MaxAssetsWeightStr` field in a format suitable for display. Possible values: • `Unknown` • `Low` • `Medium` • `High` • `Critical`
`IntegrationID`	String	ID of the alert in the IRP / SOAR application, if integration with such an application is configured in KUMA.
`ExternalReference`	String	Link to a section in the IRP / SOAR application that displays information about an alert imported from KUMA.
`IncidentID`	String	ID of the incident to which the alert is linked.
`IncidentName`	String	Name of the incident to which the alert is linked.
`SegmentationRuleName`	String	Name of the segmentation rule used to group correlation events in the alert.
`BranchID`	String	ID of the hierarchy branch in which the alert was generated. Indicated for a hierarchical deployment of KUMA.
`BranchName`	String	Name of the hierarchy branch in which the alert was generated. Indicated for a hierarchical deployment of KUMA.
`Actions`	Nested `[Action]` structure	Nested structure with lines indicating changes to alert statuses and assignments, and user comments.
`Events`	Nested `[EventWrapper]` structure	Nested structure from which you can query the correlation events associated with the alert.
`Assets`	Nested `[Asset]` structure	Nested structure from which you can query assets associated with the alert.
`Accounts`	Nested `[Account]` structure	Nested structure from which you can query the user accounts associated with the alert.
`AffectedAssets`	Nested `[Affected]` structure	Nested structure from which you can query alert-related assets and user accounts, and find out the number of times they appear in alert events.

Nested `Affected` structure

Field	Data type	Description
`Assets`	Nested `[AffectedRecord]` list	List and number of assets associated with the alert.
`Accounts`	Nested `[AffectedRecord]` list	List and number of user accounts associated with the alert.

Nested `AffectedRecord` structure

Field	Data type	Description
`Value`	String	ID of the asset or user account.
`Count`	Number	The number of times an asset or user account appears in alert-related events.

Nested `EventWrapper` structure

Field	Data type	Description
`Event`	Nested `[Event]` structure	Event fields.
`Comment`	String	Comment added when events were added to the alert.
`LinkedAt`	Number	Date when events were added to the alert.

Nested `Action` structure

Field	Data type	Description
`CreatedAt`	Number	Date when the action was taken on the alert.
`UserID`	String	User ID.
`Kind`	String	Type of action.
`Value`	String	Value.
`Event`	Nested `[Event]` structure	Event fields.
`ClusterID`	String	Cluster ID.

Asset data model

The structure of an asset is represented by fields that contain values. Fields can also contain nested structures.

Asset field	Value type	Description
`ID`	String	Asset ID.
`TenantName`	String	Tenant name.
`DeletedAt`	Number	Asset deletion date.
`CreatedAt`	Number	Asset creation date.
`TenantID`	String	Tenant ID.
`DirectCategories`	Nested list of strings	Asset categories.
`CategoryModels`	Nested `[Category]` structure	Changes asset categories.

`AffectedByIncidents`	Nested dictionary: `[string:string TRUE/FALSE]`	IDs of incidents.
`IPAddress`	Nested list of strings	Asset IP addresses.
`FQDN`	String	Asset FQDN.
`Weight`	Number	Asset importance.
`Deleted`	String with `TRUE/FALSE` values	Indicator of whether the asset has been marked for deletion from KUMA.
`UpdatedAt`	Number	Date of last update of the asset.
`MACAddress`	Nested list of strings	Asset MAC addresses.
`IPAddressInt`	Nested list of numbers	IP address in number format.
`Owner`	Nested `[OwnerInfo]` structure	Asset owner information.
`OS`	Nested `[OS]` structure	Asset operating system information.
`displayName`	String	Asset name.
`APISoft`	Nested `[Software]` structure	Software installed on the asset.
`APIVulns`	Nested `[Vulnerability]` structure	Asset vulnerabilities.
`KICSServerIp`	String	KICS/KATA server IP address.
`KICSConnectorID`	Number	KICS/KATA connector ID.
`KICSDeviceID`	Number	KICS/KATA asset ID.
`KICSStatus`	String	KICS/KATA asset status.
`KICSHardware`	Nested `[KICSSystemInfo]` structure	Asset hardware information received from KICS/KATA.
`KICSSoft`	Nested `[KICSSystemInfo]` structure	Asset software information received from KICS/KATA.
`KICSRisks`	Nested `[KICSRisk]` structure	Asset vulnerability information received from KICS/KATA.
`Sources`	Nested `[Sources]` structure	Basic information about the asset from various sources.
`FromKSC`	String with `TRUE/FALSE` values	Indicator that asset details have been imported from KSC.
`NAgentID`	String	ID of the KSC Agent from which the asset information was received.
`KSCServerFQDN`	String	FQDN of the KSC Server.
`KSCInstanceID`	String	KSC instance ID.
`KSCMasterHostname`	String	KSC Server host name.
`KSCGroupID`	Number	KSC group ID.
`KSCGroupName`	String	KSC group name.
`LastVisible`	Number	Date when information about the asset was last received from KSC.
`Products`	Nested dictionary: `[string:nested [ProductInfo] structure]`	Information about Kaspersky applications installed on the asset received from KSC.
`Hardware`	Nested `[Hardware]` structure	Asset hardware information received from KSC.
`KSCSoft`	Nested `[Software]` structure	Asset software information received from KSC.
`KSCVulns`	Nested `[Vulnerability]` structure	Asset vulnerability information received from KSC.

Nested `Category` structure

Field	Value type	Description
`ID`	String	Category ID.
`TenantID`	String	Tenant ID.
`TenantName`	String	Tenant name.
`Parent`	String	Parent category.
`Path`	Nested list of strings	Structure of categories.
`Name`	String	Category name.
`UpdatedAt`	Number	Last update of the category.
`CreatedAt`	Number	Category creation date.
`Description`	String	Category description.
`Weight`	Number	Category importance.
`CategorizationKind`	String	Asset category assignment type.
`CategorizationAt`	Number	Categorization date.
`CategorizationInterval`	String	Category assignment interval.

Nested `OwnerInfo` structure

Field	Value type	Description
`displayName`	String	Name of the asset owner.

Nested `OS` structure

Field	Value type	Description
`Name`	String	Name of the operating system.
`BuildNumber`	Number	Operating system version.

Nested `Software` structure

Field	Value type	Description
`displayName`	String	Software name.
`DisplayVersion`	String	Software version.
`Publisher`	String	Software publisher.

`InstallDate`	String	Installation date.
`HasMSIInstaller`	`TRUE/FALSE` string	Indicates whether the software has an MSI installer.

Nested `Vulnerability` structure

Field	Value type	Description
`KasperskyID`	String	Vulnerability ID assigned by Kaspersky.
`ProductName`	String	Software name.
`DescriptionURL`	String	URL containing the vulnerability description.
`RecommendedMajorPatch`	String	Recommended update.
`RecommendedMinorPatch`	String	Recommended update.
`SeverityStr`	String	Vulnerability severity.
`Severity`	Number	Vulnerability severity.
`CVE`	Nested list of strings	CVE vulnerability ID.
`ExploitExists`	`TRUE/FALSE` string	Indicates whether an exploit exists.
`MalwareExists`	`TRUE/FALSE` string	Indicates whether malware exists.

Nested `KICSSystemInfo` structure

Field	Value type	Description
`Model`	String	Device model.
`Version`	String	Device version.
`Vendor`	String	Vendor.

Nested `KICSRisk` structure

Field	Value type	Description
`ID`	Number	KICS/KATA risk ID.
`Name`	String	Risk name.
`Category`	String	Risk type.
`Description`	String	Risk description.
`DescriptionURL`	String	Link to risk description.
`Severity`	Number	Risk severity.
`Cvss`	Number	CVSS score.

Nested `Sources` structure

Field	Value type	Description
`KSC`	Nested `[SourceInfo]` structure	Asset information received from KSC.
`API`	Nested `[SourceInfo]` structure	Asset information received through the REST API.
`Manual`	Nested `[SourceInfo]` structure	Manually entered information about the asset.
`KICS`	Nested `[SourceInfo]` structure	Asset information received from KICS/KATA.

Nested `Sources` structure

Field	Value type	Description
`MACAddress`	Nested list of strings	Asset MAC addresses.
`IPAddressInt`	Nested list of numbers	IP address in number format.
`Owner`	Nested `[OwnerInfo]` structure	Asset owner information.
`OS`	Nested `[OS]` structure	Asset operating system information.
`displayName`	String	Asset name.
`IPAddress`	Nested list of strings	Asset IP addresses.
`FQDN`	String	Asset FQDN.
`Weight`	Number	Asset importance.
`Deleted`	String with `TRUE/FALSE` values	Indicator of whether the asset has been marked for deletion from KUMA.
`UpdatedAt`	Number	Date of last update of the asset.

Nested structure `ProductInfo`

Field	Value type	Description
`ProductVersion`	String	Software version.
`ProductName`	String	Software name.

Nested `Hardware` structure

Field	Value type	Description
`NetCards`	Nested `[NetCard]` structure	List of network cards of the asset.
`CPU`	Nested `[CPU]` structure	List of asset processors.
`RAM`	Nested `[RAM]` structure	Asset RAM list.
`Disk`	Nested `[Disk]` structure	List of asset drives.

Nested `NetCard` structure

Field	Value type	Description
`ID`	String	Network card ID.
`MACAddresses`	Nested list of strings	MAC addresses of the network card.
`Name`	String	Network card name.
`Manufacture`	String	Network card manufacture.
`DriverVersion`	String	Driver version.

Nested `RAM` structure

Field	Value type	Description
`Frequency`	String	RAM frequency.
`TotalBytes`	Number	Amount of RAM, in bytes.

Nested `CPU` structure

Field	Value type	Description
`ID`	String	CPU ID.
`Name`	String	CPU name.
`CoreCount`	String	Number of cores.
`CoreSpeed`	String	Frequency.

Nested `Disk` structure

Field	Value type	Description
`FreeBytes`	Number	Available disk space.
`TotalBytes`	Number	Total disk space.

User account data model

User account fields can be addressed from email templates and during event correlation.

Field	Value type	Description
`ID`	String	User account ID.

ObjectGUID	String	Active Directory attribute. User account ID in Active Directory.
TenantID	String	Tenant ID.
TenantName	String	Tenant name.
UpdatedAt	Number	Last update of user account.
Domain	String	Domain.
CN	String	Active Directory attribute. User name.
displayName	String	Active Directory attribute. Displayed user name.
DistinguishedName	String	Active Directory attribute. LDAP object name.
employeeID	String	Active Directory attribute. Employee ID.
Mail	String	Active Directory attribute. User email address.
mailNickname	String	Active Directory attribute. Alternate email address.
Mobile	String	Active Directory attribute. Mobile phone number.
ObjectSID	String	Active Directory attribute. Security ID.
SAMAccountName	String	Active Directory attribute. Login.
TelephoneNumber	String	Active Directory attribute. Phone number.
UserPrincipalName	String	Active Directory attribute. User principal name (UPN).
Archived	TRUE/FALSE string	Indicator that determines whether a user account is obsolete.
MemberOf	List of strings	Active Directory attribute. AD groups joined by the user. This attribute can be used for an event search during correlation.
PreliminarilyArchived	TRUE/FALSE string	Indicator that determines whether a user account should be designated as obsolete.
CreatedAt	Number	User account creation date.
SN	String	Active Directory attribute. Last name of the user.
SAMAccountType	String	Active Directory attribute. User account type.
Title	String	Active Directory attribute. Job title of the user.
Division	String	Active Directory attribute. User's department.
Department	String	Active Directory attribute. User's division.
Manager	String	Active Directory attribute. User's supervisor.
Location	String	Active Directory attribute. User's location.
Company	String	Active Directory attribute. User's company.
StreetAddress	String	Active Directory attribute. Company address.
PhysicalDeliveryOfficeName	String	Active Directory attribute. Delivery address.
managedObjects	List of strings	Active Directory attribute. Objects under control of the user.
UserAccountControl	Number	Active Directory attribute. AD account type.
WhenCreated	Number	Active Directory attribute. User account creation date.
WhenChanged	Number	Active Directory attribute. User account modification date.
AccountExpires	Number	Active Directory attribute. User account expiration date.
BadPasswordTime	Number	Active Directory attribute. Date of last unsuccessful login attempt.

KUMA audit events

Audit events are created when certain security-related actions are completed in KUMA. These events are used to ensure system integrity.

Audit events are created on the KUMA Core server and sent to the storage of the Main tenant the correlators of the Main tenant. Therefore, at least one storage must be created in the Main tenant for storing audit events. If no storage exists, you need to create one. Audit events are sent to the KUMA Audit space, which is created automatically inside the storage.

To view audit events, you need to go to the **Events** section in KUMA and add `SELECT * FROM 'events' WHERE Type=4` to the query.

As a result of executing the query, audit events are displayed if the user role allows viewing audit events.

Event fields with general information

Every audit event has the event fields described in the table below.

Event field name	Field value
`Timestamp`	Event time.
`DeviceHostName`	The event source host. For audit events, the hostname is the hostname of the host where the kuma-core service is installed because the service is the source of events.
`DeviceTimeZone`	Timezone of the system time of the server hosting the KUMA Core in the format `+-hh:mm`.
`Type`	Type of the audit event. `Audit` or `Base`.
`TenantID`	Tenant ID.
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`EndTime`	Event creation time.
`SpaceID`	`KUMA Audit`
`DeviceAction`	The action captured in the audit event.

User was successfully signed in or failed to sign in

Event field name	Field value
`DeviceAction`	`user login`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.

SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login.
SourceUserID	User ID.
Message	Description of the error. Appears only if an error occurred during login. Otherwise, the field will be empty.

User login changed

Event field name	Field value
DeviceAction	user login changed
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
DestinationUserName	User login whose data was changed.
DestinationUserID	ID of the user whose data was changed.
DeviceCustomString1	Current value of the login.
DeviceCustomString1Label	new login
DeviceCustomString2	Value of the login before it was changed.
DeviceCustomString2Label	old login

Other data of the user was changed

Event field name	Field value
DeviceAction	user other info changed
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
DestinationUserName	User login whose data was changed.
DestinationUserID	ID of the user whose data was changed.

User logged out

This event appears only when the user pressed the logout button.

This event will not appear if the user is logged out due to the end of the session or if the user logs in again from another browser.

Field values of audit event User logged out

Event field name	Field value
`DeviceAction`	`user logout`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User login.
`SourceUserID`	User ID.

User password was changed

Event field name	Field value
`DeviceAction`	`user password changed`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that modified the data.
`SourceUserID`	ID of the user that modified the data.
`DestinationUserName`	User login whose data was changed.
`DestinationUserID`	ID of the user whose data was changed.

User was created

Event field name	Field value
`DeviceAction`	`user created`
`EventOutcome`	`succeeded`

SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that created the user account.
SourceUserID	ID of the user that created the user account.
DestinationUserName	User login for which the user account was created.
DestinationUserID	User ID for which the user account was created.
DeviceCustomString1	Role of the created user.
DeviceCustomString1Label	`role`

User role was assigned

Event field name	Field value
DeviceAction	`granted access`
EventOutcome	`succeeded`
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user whose data was changed.
SourceUserID	ID of the user whose data was changed.
DestinationUserPrivileges	Role ID of the user whose data was changed.
DeviceCustomString5	ID of the tenant used to assign the role.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	`tenant name`

User role was revoked

Event field name	Field value
DeviceAction	`revoked access`
EventOutcome	`succeeded`
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

SourceUserName	Login of the user that made the changes.
SourceUserID	ID of the user that made the changes.
DestinationUserName	User login whose data was changed.
DestinationUserID	ID of the user whose data was changed.
DestinationUserPrivileges	Role ID of the user whose data was changed.
DeviceCustomString5	ID of the tenant used to assign the role.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

The user has edited the set of fields settings to define sources

Event field name	Field value
DeviceAction	settings updated
DeviceFacility	eventSourceIdentity
EventOutcome	succeeded
SourceUserName	Login of the user that made the changes.
SourceUserID	ID of the user that made the changes.
DeviceCustomString5	Updated set of fields, | is used as the delimiter.

Alert assigned to the user

Event field name	Field value
DeviceAction	user is assigned to alert
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that assigned the alert to the user.
SourceUserID	ID of the user that assigned the alert to the user.
ExternalID	Alert ID.
Name	Alert name.
DestinationUserName	User name of the user to which the alert was assigned.
DestinationUserID	ID of the user to which the alert was assigned.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

User access token was changed

Event field name	Field value
DeviceAction	user access token changed
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
DestinationUserName	User login whose data was changed.
DestinationUserID	ID of the user whose data was changed.

Key file added

Event field name	Field value
DeviceAction	license key installed
EventOutcome	succeeded
Message	License name.
SourceUserID	ID of the user that added the key file.
SourceUserName	User name of the user that added the key file.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Application activated with an activation code

Event field name	Field value
DeviceAction	license activated
EventOutcome	succeeded
Message	License name.
SourceUserID	ID of the user that entered the activation code.

SourceUserName	User name of the user that entered the activation code.
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Reserve license key added

Event field name	Field value
DeviceAction	`reserve license key installed`
DeviceAddress	IP address of the device on which the reserve license key was added.
EventOutcome	`succeeded`
Message	License name.
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserID	ID of the user that added the reserve license key.
SourceUserName	User name of the user that added the reserve license key.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	`tenant name`

Reserve license key deleted

Event field name	Field value
DeviceAction	`reserve license key uninstalled`
DeviceAddress	IP address of the device on which the reserve license key was deleted.
EventOutcome	`succeeded`
Message	License name.
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserID	ID of the user that deleted the reserve license key.
SourceUserName	User name of the user that deleted the reserve license key.

DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

The license is renewed

Event field name	Field value
DeviceAction	license reactivated
EventOutcome	succeeded
Message	License name.
SourceUserID	ID of the user that added the key file.
SourceUserName	User name of the user that added the key file.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Invalid activation code

Event field name	Field value
DeviceAction	activation code license activated
EventOutcome	failed
Message	Error text.
SourceUserID	ID of the user that entered the activation code.
SourceUserName	User name of the user that entered the activation code.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Activation code blocked

Event field name	Field value
DeviceAction	Activation code blocked
EventOutcome	succeeded
Message	License name.

`SourceUserID`	ID of the user that entered the activation code.
`SourceUserName`	User name of the user that entered the activation code.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Activation code or key file deleted

Event field name	Field value
`DeviceAction`	`Activation code or key file uninstalled`
`EventOutcome`	`succeeded`
`Message`	License name.
`SourceUserID`	ID of the user that deleted the key file.
`SourceUserName`	User name of the user that deleted the key file.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Activation code or key file replaced

Event field name	Field value
`DeviceAction`	`Activation code or key file replaced`
`EventOutcome`	`succeeded`
`Message`	License name.
`SourceUserID`	ID of the user that performed the replacement.
`SourceUserName`	User name of the user that performed the replacement.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

EPS exceeded

Event field name	Field value
`DeviceAction`	`license limit for EPS exceeded`
`EventOutcome`	`succeeded`
`Message`	License name.
`SourceUserID`	ID of the user that added the key file or entered the activation code.
`SourceUserName`	User name of the user that added the key file or entered the activation code.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

License expiration and start of grace period

Event field name	Field value
`DeviceAction`	`license expired`
`EventOutcome`	`succeeded`
`Message`	License name.
`SourceUserID`	ID of the user that added the key file or entered the activation code.
`SourceUserName`	User name of the user that added the key file or entered the activation code.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

End of grace period

Event field name	Field value
`DeviceAction`	`license ended`
`EventOutcome`	`succeeded`
`Message`	License name.
`SourceUserID`	ID of the user that added the key file or entered the activation code.
`SourceUserName`	User name of the user that added the key file or entered the activation code.
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.

SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

Expired activation code or key file added

Event field name	Field value
DeviceAction	Activation code or key file installed
IP	The IP address at which the key file has been added or activation code has been entered.
EventOutcome	failed
Message	Error text.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserID	ID of the user that added the key file or entered the activation code.
SourceUserName	User name of the user that added the key file or entered the activation code.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Changed the set of spaces to differentiate access to events

Event field name	Field value
DeviceAction	• space set was created • space set was deleted • space set was updated (including granting and revoking access permissions)
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the settings.
SourceUserID	ID of the user that modified the settings.
DeviceCustomString5	ID of the space set.
DeviceCustomString5Label	set ID
DeviceCustomString3	Name of the space set.
DeviceCustomString3Label	space name

Service monitoring thresholds changed

Event field name	Field value
DeviceAction	settings updated
DeviceFacility	serviceAlertSettings
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the settings.
SourceUserID	ID of the user that modified the settings.
DeviceCustomString1	JSON with threshold values recorded in the database.
DeviceCustomString1Label	thresholds
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

KUMA Core settings modified

Event field name	Field value
DeviceAction	settings updated
DeviceFacility	coreProperties
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the settings.
SourceUserID	ID of the user that modified the settings.
DeviceCustomString1	JSON with the values of the KUMA Core settings recorded in the database.
DeviceCustomString1Label	properties

GeoIP databases imported

Event field name	Field value
`DeviceAction`	`new geobase imported`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that imported the databases.
`SourceUserID`	ID of the user that imported the databases.
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Service was created

Event field name	Field value
`DeviceAction`	`service created`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that created the service.
`SourceUserID`	ID of the user that created the service.
`DeviceExternalID`	Service ID.
`DeviceProcessName`	Service name.
`DeviceFacility`	Service type.
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Service was deleted

Event field name	Field value
DeviceAction	service deleted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that deleted the service.
SourceUserID	ID of the user that deleted the service.
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DestinationAddress	Address of the device that was used to start the service. If the service has never been started before, the field will be empty.
DestinationHostName	The FQDN of the machine that was used to start the service. If the service has never been started before, the field will be empty.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Service was reloaded

Event field name	Field value
DeviceAction	service reloaded
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that restarted the service.
SourceUserID	ID of the user that restarted the service.
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DeviceCustomString5	Tenant ID.

DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Service was restarted

Event field name	Field value
DeviceAction	service restarted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that restarted the service.
SourceUserID	ID of the user that restarted the service.
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Service was started

Event field name	Field value
DeviceAction	service started
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DestinationAddress	Address of the device where the service was started.
DestinationHostName	FQDN of the device where the service was started.
DeviceCustomString5	Tenant ID.

DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Service was paired

Event field name	Field value
DeviceAction	service paired
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Service status was changed

Event field name	Field value
DeviceAction	service status changed
DeviceExternalID	Service ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DestinationAddress	Address of the device where the service was started.
DestinationHostName	FQDN of the device where the service was started.
DeviceCustomString1	green, yellow, or red
DeviceCustomString1Label	new status
DeviceCustomString2	green, yellow, or red
DeviceCustomString2Label	old status
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Partition was deleted by user

Event field name	Field value
DeviceAction	partition deleted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that deleted the partition.
SourceUserID	ID of the user that deleted the partition.
Name	Storage name | Tenant of the partition being moved or deleted | Name of the space to which the partition belongs.
DeviceCustomDate1	Data modification time (UTC). The date that is displayed in the storage partitions in the `date` column.
DeviceCustomDate1Label	date of event
Message	deleted by user

Partition automatically deleted after retention period

Event field name	Field value
DeviceAction	partition deleted
EventOutcome	succeeded
Name	Name of the space to which the partition belongs.
DeviceCustomDate1	Data modification time (UTC). The date that is displayed in the storage partitions in the 'date' column.
DeviceCustomDate1Label	date of event
SourceServiceName	scheduler
Message	deleted by retention period settings

Partition deleted by absolute retention period

Event field name	Field value
Name	Name of the space to which the partition belongs.
Message	deleted partition data
DeviceAction	applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Data modification time (UTC). The date that is displayed in the storage partitions in the 'date' column.
DeviceCustomDate1Label	date of partition

DeviceCustomNumber1	Partition size.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Number of events.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Partition deleted by relative retention period

Event field name	Field value
Name	Name of the space to which the partition belongs.
Message	deleted partition data
DeviceAction	applied retention policy by percent
SourceServiceName	scheduler
DeviceCustomDate1	Data modification time (UTC). The date that is displayed in the storage partitions in the 'date' column.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Partition size.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Number of events.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Partition moved to cold storage

Event field name	Field value
Name	Name of the space to which the partition belongs.
Message	moved partition data to cold storage
DeviceAction	The following values are available: • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Data modification time (UTC). The date that is displayed in the storage partitions in the 'date' column.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Partition size.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Number of events.
DeviceCustomNumber2Label	events
EventOutcome	succeeded
DeviceCustomString1	ID of the space.
DeviceCustomString1Label	nodeID

Error moving partition to cold storage

Event field name	Field value
`Name`	Name of the space to which the partition belongs.
`Message`	`move partition data to cold storage failed: {"error":"Code: 243. DB::Exception: Move is not possible. Not enough space on 'cold_volume'. (NOT_ENOUGH_SPACE) (version 23.8.8.207)\n"}`
`DeviceAction`	The following values are available: • `applied retention policy by days` • `applied retention policy by percent` • `applied retention policy by GB`
`SourceServiceName`	`scheduler`
`DeviceCustomDate1`	Data modification time (UTC). The date that is displayed in the storage partitions in the 'date' column.
`DeviceCustomDate1Label`	`date of partition`
`DeviceCustomNumber1`	Partition size.
`DeviceCustomNumber1Label`	`size`
`DeviceCustomNumber2`	Number of events.
`DeviceCustomNumber2Label`	`events`
`EventOutcome`	`failed`
`DeviceCustomString1`	ID of the space.
`DeviceCustomString1Label`	`nodeID`

Active list was successfully cleared or operation failed

Audit events for active lists are created only for actions performed by users. Audit events are not generated when the active lists are modified using correlation rules. **If you need to track such changes, you can do so using alerts**.

If an active list is modified using a correlation rule of the **simple** type, in which the **Output** and **Loop** actions are defined, an active list modification alert will be created each time the rule is triggered.

The event can be assigned the `succeeded` or `failed` status.

Since the request to clear an active list is made over a remote connection, a data transfer error may occur at any moment: both before and after deletion.

This means that the active list may be cleared successfully, but the event is assigned the `failed` status, because EventOutcome returns the TCP/IP connection status of the request, but not the succeeded or failed status of the active list clearing.

Field values of audit event "Active list was successfully cleared or operation failed"

Event field name	Field value
`DeviceAction`	`active list cleared`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.

`SourcePort`	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
`SourceUserName`	User login that was used to clear the active list.
`SourceUserID`	User ID that was used to clear the active list.
`DeviceExternalID`	Service ID whose active list was cleared.
`ExternalID`	Active list ID.
`Name`	Active list name.
`Message`	If EventOutcome = `failed`, an error message can be found here.
`DeviceCustomString5`	Service tenant ID. Some errors prevent adding tenant information to the event.
`DeviceCustomString5Label`	tenant ID
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	tenant name

Active list item was successfully changed, or operation was unsuccessful

Audit events for active lists are created only for actions performed by users. Audit events are not generated when the active lists are modified using correlation rules. **If you need to track such changes, you can do so using alerts**.

If an active list is modified using a correlation rule of the **simple** type, in which the **Output** and **Loop** actions are defined, an active list modification alert will be created each time the rule is triggered.

The event can be assigned the `succeeded` or `failed` status.

Since the request to change an active list item is made over a remote connection, a data transfer error may occur at any moment: both before and after the change.

This means that the active list item may be changed successfully, but the event is assigned the `failed` status, because EventOutcome returns the TCP/IP connection status of the request, but not the succeeded or failed status of the active list item change.

Field values of audit event "Active list item was successfully changed, or operation was unsuccessful"

Event field name	Field value
`DeviceAction`	`active list item changed`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User login used to change the active list item.
`SourceUserID`	User ID used to change the active list item.
`DeviceExternalID`	Service ID for which the active list is changed.
`ExternalID`	Active list ID.
`Name`	Active list name.
`DeviceCustomString1`	Key name.

DeviceCustomString1Label	key
Message	If EventOutcome = failed, an error message can be found here.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name
DeviceCustomString6Label	tenant name

Active list item was successfully deleted or operation was unsuccessful

Audit events for active lists are created only for actions performed by users. Audit events are not generated when the active lists are modified using correlation rules. **If you need to track such changes, you can do so using alerts**.

If an active list is modified using a correlation rule of the **simple** type, in which the **Output** and **Loop** actions are defined, an active list modification alert will be created each time the rule is triggered.

The event can be assigned the `succeeded` or `failed` status.

Since the request to delete an active list item is made over a remote connection, a data transfer error may occur at any moment: both before and after deletion.

This means that the active list item may be deleted successfully, but the event is assigned the `failed` status, because EventOutcome returns the TCP/IP connection status of the request, but not the succeeded or failed status of the active list item deletion.

Field values of audit event "Active list item was successfully deleted or operation was unsuccessful"

Event field name	Field value
DeviceAction	active list item deleted
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to delete the item from the active list.
SourceUserID	User ID that was used to delete the item from the active list.
DeviceExternalID	Service ID whose active list was cleared.
ExternalID	Active list ID.
Name	Active list name.
DeviceCustomString1	Key name.
DeviceCustomString1Label	key
Message	If EventOutcome = failed, an error message can be found here.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Active list was successfully imported or operation failed

Audit events for active lists are created only for actions performed by users. Audit events are not generated when the active lists are modified using correlation rules. **If you need to track such changes, you can do so using alerts**.

If an active list is modified using a correlation rule of the **simple** type, in which the **Output** and **Loop** actions are defined, an active list modification alert will be created each time the rule is triggered.

Active list items are imported in parts via a remote connection.

Since the import is performed via a remote connection, a data transfer error can occur at any time: when the data is imported partially or completely. EventOutcome returns the connection status, not the import status.

Field values of audit event "Active list was successfully imported or operation failed"

Event field name	Field value
DeviceAction	active list imported
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to perform the import.
SourceUserID	User ID that was used to perform the import.
DeviceExternalID	Service ID for which an import was performed.
ExternalID	Active list ID.
Name	Active list name.
Message	If EventOutcome = failed, an error message can be found here. The error text can be in json format, for example, {"error":"line 1: header does not contain column IP!"}.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name
DeviceCustomString6Label	tenant name

Active list was exported

Audit events for active lists are created only for actions performed by users. Audit events are not generated when the active lists are modified using correlation rules. **If you need to track such changes, you can do so using alerts**.

If an active list is modified using a correlation rule of the **simple** type, in which the **Output** and **Loop** actions are defined, an active list modification alert will be created each time the rule is triggered.

Field values of audit event "Active list was exported"

Event field name	Field value
DeviceAction	active list exported
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to perform the export.
SourceUserID	User ID that was used to perform the export.
DeviceExternalID	Service ID for which an export was performed.
ExternalID	Active list ID.
Name	Active list name.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name
DeviceCustomString6Label	tenant name

Context table exported

Audit events for context tables are created only for actions performed by users.

Field values of audit event "Context table exported"

Event field name	Field value
DeviceAction	context table exported
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to perform the export.
SourceUserID	User ID that was used to perform the export.
DeviceExternalID	Service ID for which an export was performed.
ExternalID	Context table ID
Name	Name of the context table.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Context table successfully imported or operation failed

Audit events for context tables are created only for actions performed by users.

Context table items are imported in parts via a remote connection.

Since the import is performed via a remote connection, a data transfer error can occur at any time: when the data is imported partially or completely. EventOutcome returns the connection status, not the import status.

Field values of audit event "Context table successfully imported or operation failed"

Event field name	Field value
`DeviceAction`	`context table imported`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User login that was used to perform the import.
`SourceUserID`	User ID that was used to perform the import.
`DeviceExternalID`	Service ID for which an import was performed.
`ExternalID`	Context table ID
`Name`	Name of the context table.
`Message`	If EventOutcome = `failed`, an error message can be found here.
`DeviceCustomString5`	Service tenant ID. Some errors prevent adding tenant information to the event.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Context table item successfully modified or operation failed

Audit events for context tables are created only for actions performed by users.

The event can be assigned the `succeeded` or `failed` status.

Field values of audit event "Context table item successfully modified or operation failed"

Event field name	Field value
`DeviceAction`	`context table item is set`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.

`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that changed the context table item.
`SourceUserID`	ID of the user that changed the context table item.
`DeviceExternalID`	ID of the service whose context table was modified.
`ExternalID`	Context table ID
`Name`	Name of the context table.
`DeviceCustomString1`	Name of the record key.
`DeviceCustomString1Label`	`key`
`Message`	If EventOutcome = `failed`, an error message can be found here.
`DeviceCustomString5`	Service tenant ID. Some errors prevent adding tenant information to the event.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Context table item successfully deleted or operation failed

Audit events for context tables are created only for actions performed by users.

The event can be assigned the `succeeded` or `failed` status.

Field values of audit event "Context table item modified or operation failed"

Event field name	Field value
`DeviceAction`	`context table item deleted`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that deleted the context table item.
`SourceUserID`	ID of the user that deleted the context table item.
`DeviceExternalID`	ID of the service for which the context table item was deleted.
`ExternalID`	Context table ID
`Name`	Name of the context table.
`DeviceCustomString1`	Name of the record key.
`DeviceCustomString1Label`	`key`
`Message`	If EventOutcome = `failed`, an error message can be found here.
`DeviceCustomString5`	Service tenant ID. Some errors prevent adding tenant information to the event.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Context table successfully cleared or operation failed

Audit events for context tables are created only for actions performed by users.

The event can be assigned the `succeeded` or `failed` status.

Since the request to clear a context table is made over a remote connection, a data transfer error may occur at any moment: both before and after deletion.

This means that the context table may be cleared successfully, but the event gets the `failed` status anyway, because EventOutcome returns the TCP/IP connection status of the request, but not the succeeded or failed status of the context table clearing.

Field values of audit event "Context table successfully cleared or operation failed"

Event field name	Field value
`DeviceAction`	`context table cleared`
`EventOutcome`	`succeeded` or `failed`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that cleared the context table.
`SourceUserID`	ID of the user that cleared the context table.
`DeviceExternalID`	ID of the service whose context table was cleared.
`ExternalID`	Context table ID
`Name`	Name of the context table.
`Message`	If EventOutcome = `failed`, an error message can be found here.
`DeviceCustomString5`	Service tenant ID. Some errors prevent adding tenant information to the event.
`DeviceCustomString5Label`	tenant ID
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	tenant name

Resource was added

Event field name	Field value
`DeviceAction`	`resource added`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.

SourceUserName	User login that was used to add the resource.
SourceUserID	User ID that was used to add the resource.
DeviceExternalID	Resource ID.
DeviceProcessName	Resource name.
DeviceFacility	Resource type: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Resource was deleted

Event field name	Field value
DeviceAction	resource deleted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to delete the resource.
SourceUserID	User ID that was used to delete the resource.
DeviceExternalID	Resource ID.
DeviceProcessName	Resource name.

`DeviceFacility`	Resource type: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Resource was updated

Event field name	Field value
`DeviceAction`	`resource updated`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User login that was used to update the resource.
`SourceUserID`	User ID that was used to update the resource.
`DeviceExternalID`	Resource ID.
`DeviceProcessName`	Resource name.
`DeviceFacility`	Resource type: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`

DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Importing resources

Event field name	Field value
DeviceAction	import resources
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that imported the resources.
SourceUserID	ID of the user that imported the resources.
DeviceCustomString5	ID of the tenant into which the resources were imported.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Name of the tenant into which the resources were imported.
DeviceCustomString6Label	tenant name
FileType	Import source: file or repository.
FileID	If resources are imported from a repository, the package ID. If resources are imported from a file, the system ID of the file.
ExternalID	If resources are imported from a repository, the version of the imported package. If resources are imported from a file, empty value.

Asset was created

Event field name	Field value
DeviceAction	asset created
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to add the asset.
SourceUserID	User ID that was used to add the asset.
DeviceAssetID	Asset ID.
SourceHostName	Asset ID.
Name	Asset name.
DeviceCustomString1	Comma-separated IP addresses of the asset.
DeviceCustomString1Label	addresses

DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Asset was deleted

Event field name	Field value
DeviceAction	asset deleted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to add the asset.
SourceUserID	User ID that was used to add the asset.
DeviceAssetID	Asset ID.
SourceHostName	Asset ID.
Name	Asset name.
DeviceCustomString1	Comma-separated IP addresses of the asset.
DeviceCustomString1Label	addresses
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Asset category was added

Event field name	Field value
DeviceAction	category created
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to add the category.
SourceUserID	User ID that was used to add the category.
DeviceExternalID	Category ID.

Name	Category name.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Asset category was deleted

Event field name	Field value
DeviceAction	category deleted
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to delete the category.
SourceUserID	User ID that was used to delete the category.
DeviceExternalID	Category ID.
Name	Category name.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Settings were updated

Event field name	Field value
DeviceAction	settings updated
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login that was used to update the settings.
SourceUserID	User ID that was used to update the settings.
DeviceFacility	Type of settings.
DeviceCustomString1	JSON with threshold values recorded in the database.
DeviceCustomString5	Tenant ID.

DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Tenant was created

Event field name	Field value
DeviceAction	tenant created
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User login used to create the tenant.
SourceUserID	User ID used to create the tenant.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Tenant was enabled

Event field name	Field value
DeviceAction	tenant enabled
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User login used to enable the tenant.
SourceUserID	User ID used to enable the tenant.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Tenant was disabled

Event field name	Field value
DeviceAction	tenant disabled
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User login used to disable the tenant.
SourceUserID	User ID used to disable the tenant.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Other tenant data was changed

Event field name	Field value
DeviceAction	tenant other info changed
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User login that was used to change the tenant data.
SourceUserID	User ID that was used to change the tenant data.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

The dictionary was successfully updated on the service or operation was unsuccessful

Event field name	Field value
DeviceAction	dictionary update succeeded
EventOutcome	succeeded or failed

`SourceTranslatedAddress`	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
`SourceUserName`	User login that was used to create the service.
`SourceUserID`	User ID that was used to create the service.
`DeviceExternalID`	Service ID.
`ExternalID`	Dictionary ID.
`DeviceProcessName`	Service name.
`DeviceFacility`	Service type.
`DeviceCustomString1`	Dictionary type: table, dictionary.
`DeviceCustomString1Label`	`dictionary type`
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`
`Message`	If EventOutcome = `failed`, an error message can be found here.

Dictionary entry added

Dictionary item added or updated via the API.

Field values of audit event "Dictionary entry added"

Event field name	Field value
`DeviceAction`	`dictionary item added`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
`SourceUserName`	User name of the user that added the item.
`SourceUserID`	ID of the user that added the item.
`DeviceExternalID`	Service ID.
`ExternalID`	Dictionary ID.
`DeviceProcessName`	Service name.
`DeviceFacility`	Service type.
`DeviceCustomString1`	Dictionary type: table, dictionary.
`DeviceCustomString1Label`	`dictionary type`
`DeviceCustomString2`	Record key.
`DeviceCustomString2Label`	`key`
`DeviceCustomString5`	Tenant ID.
`DeviceCustomString5Label`	`tenant ID`

DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Dictionary entry successfully deleted or the operation failed

Dictionary item deleted (for types: table, dictionary) via the API.

The event can be assigned the `succeeded` or `failed` status.

Field values of audit event "Dictionary entry successfully deleted or the operation failed"

Event field name	Field value
DeviceAction	dictionary item deleted
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that deleted the dictionary item.
SourceUserID	ID of the user that deleted the dictionary item.
DeviceExternalID	ID of the service whose dictionary item was deleted.
ExternalID	Dictionary ID.
DeviceProcessName	Service name.
DeviceFacility	Service type.
DeviceCustomString1	Dictionary type: table, dictionary.
DeviceCustomString1Label	dictionary type
DeviceCustomString2	Record key.
DeviceCustomString2Label	key
Message	If EventOutcome = `failed`, an error message can be found here.
DeviceCustomString5	Service tenant ID. Some errors prevent adding tenant information to the event.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Incident successfully created or operation failed

Event field name	Field value
DeviceAction	incident created
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.

SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that created the incident.
SourceUserID	ID of the user that created the incident.
ExternalID	ID of the incident.
Name	Name of the incident.
DeviceCustomString1	Alert name. This field is filled if the incident was created based of an alert. If multiple alerts were involved, these are specified as a comma-separated list.
DeviceCustomString1Label	alert name
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Incident successfully closed or operation failed

Event field name	Field value
DeviceAction	incident closed
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that closed the incident.
SourceUserID	ID of the user that closed the incident.
ExternalID	ID of the incident.
Name	Name of the incident.
DeviceCustomString1	Decision: confirmed or not confirmed.
DeviceCustomString1Label	resolution
Message	If EventOutcome = failed, an error message is written to this field.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Incident assigned to a user or operation failed

Event field name	Field value
DeviceAction	user is assigned to incident
EventOutcome	succeeded or failed

SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that assigned the user.
SourceUserID	ID of the user that assigned the user.
ExternalID	ID of the incident.
Name	Name of the incident.
DestinationUserName	User name of the user to which the incident was assigned.
DestinationUserID	ID of the user to which the incident was assigned.
Message	If EventOutcome = failed, an error message is written to this field.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Alert linked to an incident or alert unlinked from an incident, or operation failed

Event field name	Field value
DeviceAction	link alert to incident or unlink alert from incident
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that linked the alert to the incident or unlinked the alert from the incident.
SourceUserID	ID of the user that linked the alert to the incident or unlinked the alert from the incident.
ExternalID	ID of the incident.
Name	Name of the incident.
DeviceFacility	Action: link or unlink.
DeviceCustomString1	ID of the alert that was linked or unlinked.
DeviceCustomString1Label	alert ID
DeviceCustomString2	Name of the alert that was linked or unlinked.
DeviceCustomString2Label	alert name
Message	If EventOutcome = failed, an error message is written to this field.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Metrics alert registered for service or operation failed

Event field name	Field value
DeviceProcessName	Service name.
DeviceFacility	Service type.
DeviceExternalID	Service ID.
DeviceCustomString6Label	tenant name
DeviceCustomString6	Tenant name.
DeviceCustomString5Label	tenant ID
DeviceCustomString5	Tenant ID.
DeviceCustomString2Label	Possible values: • QPS threshold reached • Failed Insert QPS threshold reached • High distribution queue • Low disk space • Low disk partition space • Output Event Loss increasing • Disk buffer size increasing • Enrichment errors increasing • High enrichment queue • Connector log errors increasing
DeviceCustomString2	created (service creation time)
DeviceCustomString1Label	API port.
DeviceCustomNumber1	Duration of work in seconds.
DeviceAction	service alert
EventOutcome	succeeded or failed

Event linked to an alert or unlinked from an alert, or operation failed

Event field name	Field value
DeviceAction	link event to alert or unlink event from alert
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that linked or unlinked the event.
SourceUserID	ID of the user that linked or unlinked the event.
ExternalID	Alert ID.
Name	Alert name.
DeviceFacility	Event action: link or unlink.
DeviceCustomString1	ID of the event that was linked or unlinked.

DeviceCustomString1Label	event ID
Message	If EventOutcome = failed, an error message can be found here.
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Response in Active Directory

Event field name	Field value
DeviceAction	ad response
DeviceFacility	manual response or automatic response
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that applied the response.
SourceUserID	ID of the user that applied the response.
DeviceCustomString3	Response rule name: CHANGE_PASSWORD, ADD_TO_GROUP, REMOVE_FROM_GROUP, BLOCK_USER.
DeviceCustomString3Label	response rule name
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name
DestinationUserName	The Active Directory user account to which the response is invoked (sAMAccountName).
DestinationNtDomain	Domain of the Active Directory user account to which the response is invoked.
DestinationUserID	Account UUID in KUMA.
FlexString1	Information about the group where the user was added or deleted.
FlexString1Label	group DN

Extended event schema field created

Event field name	Field value
DeviceAction	extended field created
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that created the extended event schema field.

SourceUserID	ID of the user that created the extended event schema field.
DeviceCustomString5	Full name of the field (SA.sting_array).

Extended event schema field edited

Event field name	Field value
DeviceAction	extended field edited
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that edited the extended event schema field.
SourceUserID	ID of the user that edited the extended event schema field.
DeviceCustomString5	Full name of the field (SA.sting_array).

Extended event schema field imported

Event field name	Field value
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that imported the extended event schema field.
SourceUserID	ID of the user that imported the extended event schema field.
DeviceCustomString5	Full name of the field (SA.sting_array).

Normalizer with extended event schema field imported

Event field name	Field value
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that imported the normalizer with an extended event schema field.
SourceUserID	ID of the user that imported the normalizer with an extended event schema field.
DeviceCustomString5	Full name of the field (SA.sting_array).

Extended event schema field deleted

Event field name	Field value
DeviceAction	extended field deleted
EventOutcome	succeeded
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	User name of the user that deleted the extended event schema field.
SourceUserID	ID of the user that deleted the extended event schema field.
DeviceCustomString5	Full name of the field (SA.sting_array).

Request sent to KIRA

Event field name	Field value
DeviceAction	KIRA task
EventOutcome	succeeded/failed
SourceUserName	User login used to send the request.
SourceUserID	User ID used to send the request.
DeviceCustomString1	The resulting string that was sent.
DeviceCustomString1Label	cmd
DeviceCustomString2	ID of the event from which the request was sent.
DeviceCustomString2Label	event
DeviceCustomString3	ID of the task created to send the request.
DeviceCustomString3Label	task

KICS/KATA response

Event field name	Field value
DeviceAction	KICS response
DeviceAssetID	asset fqdn
DeviceFacility	manual response or automatic response
EventOutcome	succeeded or failed
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	Login of the user who sent the request.
SourceUserID	ID of the user who sent the request.

DeviceCustomString3	Response rule name: Authorized, Not Authorized.
DeviceCustomString3Label	response rule name
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name
DeviceExternalID	Asset ID.
SourceHostName	Asset FQDN.
Name	Asset name.
DeviceCustomString1	List of IP addresses for the asset.
DeviceCustomString1Label	addresses
Message	If EventOutcome = failed, an error message is written to this field.
DeviceCustomString2	fdqn
DeviceCustomString2Label	fqdns

Kaspersky Automated Security Awareness Platform response

Event field name	Field value
DeviceAction	KASAP response
DeviceFacility	manual response
EventOutcome	succeeded or failed
Message	Description of the error, if an error occurred, otherwise the field is empty.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	Login of the user who sent the request.
SourceUserID	ID of the user who sent the request.
DeviceCustomString1	The manager of the user to whom the course is assigned.
DeviceCustomString1Label	manager
DeviceCustomString3	Information about the group where the user belonged. Not available for failed.
DeviceCustomString3Label	manager
DeviceCustomString4	Information about the group where the user was added.
DeviceCustomString4Label	new kasap group
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name
DestinationUserID	ID of the Active Directory user account which causes the response.
DestinationUserName	Account name (sAMAccountName).
DestinationNtDomain	Domain of the Active Directory user account which causes the response.

KEDR response

Event field name	Field value
DeviceAction	KEDR response
DeviceFacility	manual response or automatic response
EventOutcome	succeeded or failed
Message	Description of the error, if an error occurred, otherwise the field is empty.
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy, there will be a proxy address.
SourcePort	Port from which the user logged in. If the user logged in using a proxy, there will be a port on the proxy side.
SourceUserName	Login of the user who sent the request.
SourceUserID	ID of the user who sent the request.
SourceAssetID	KUMA asset ID which causes the response. The value is not specified if the response is based on a hash or for all assets.
DeviceExternalID	The external ID assigned to KUMA in KEDR. If there is only one external ID, it is not filled in when started on user hosts.
DeviceCustomString1	List of IP/FQDN addresses of the asset for the host prevention rule based on the selected hash from the event card.
DeviceCustomString1Label	user defined list of ips or hostnames
DeviceCustomString2	Sensor ID parameter in KEDR (UUIDv4 | 'all' | 'custom').
DeviceCustomString2Label	sensor id of asset in KATA/EDR
ServiceID	ID of the service that caused the response. Filled in only in case of automatic response.
DeviceCustomString3	Task type name: enable_network_isolation, disable_network_isolation, enable_prevention, disable_prevention, run_process.
DeviceCustomString3Label	kedr response kind
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Importing MITRE ATT&CK techniques and tactics

Event field name	Field value
DeviceAction	import MITRE
EventOutcome	succeeded
FileID	Name of the file to import.
SourceUserID	ID of the user which sent the import request.
SourceUserName	Login of the user which sent the import request.

Backing up KUMA Core and restoring from backup

Event field name	Field value
`DeviceAction`	`backup` or `restore`
`EventOutcome`	`succeeded` or `failed`
`SourceUserName`	User name of the user that performed the backup or restoration from backup.
`SourceUserID`	ID of the user that performed the backup or restoration from backup.
`DeviceExternalID`	ID of the KUMA Core service.
`Name`	Name of the KUMA Core service.
`FilePath`	Full path at which the backup file is saved.
`Message`	If `EventOutcome = failed`, an error message can be found here.
`DeviceCustomString5`	ID of the tenant that owns the KUMA Core service.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`

Backing up partitions, restoring from backup, importing partitions from an external KUMA installation

Event field name	Field value
`DeviceAction`	`backup/restore/import`
`EventOutcome`	`succeeded` or `failed`
`SourceUserName`	User name of the user that performed partition backup, restoration from backup, import of partitions from an external KUMA installation.
`SourceUserID`	ID of the user that performed partition backup, restoration from backup, import of partitions from an external KUMA installation.
`DeviceExternalID`	ID of the storage service.
`Name`	Name of the storage.
`FilePath`	Full path at which the backup file is saved. Full path from which partitions are to be restored from backup or imported.
`Message`	If `EventOutcome = failed`, an error message can be found here.

Attempt to read events

Event field name	Field value
`DeviceAction`	`event search`
`Name`	Reading logs.
`EventOutcome`	`succeeded` or `failed`

`SourceUserName`	User name of the user that made the search query.
`SourceUserID`	ID of the user that made the search query.
`DeviceCustomString3`	List of storage spaces selected by the user in the **Events** section.
`DeviceCustomString3Label`	`space name`
`DeviceCustomString4`	Search query text.
`DeviceCustomString4Label`	`text of the search query`

The search request has been canceled

The Message field may be absent.

Event field name	Field value
`DeviceAction`	`canceling a search query`
`Message`	Reason for canceling the request.
`Name`	The search request has been canceled.
`DeviceCustomString5`	Tenant ID of the service (for some errors, information about the tenant may be absent).
`DeviceCustomString3Label`	`tenant ID`
`DeviceCustomString6`	Tenant name.
`DeviceCustomString6Label`	`tenant name`
`DeviceExternalID`	Storage ID.
`EventOutcome`	`succeeded` or `failed`
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that made the search query.
`SourceUserID`	ID of the user that made the search query.

Exporting resources from KUMA

A separate audit event is generated for each exported resource.

Event field name	Field value
`DeviceAction`	`export resources`
`EventOutcome`	`succeeded`
`SourceTranslatedAddress`	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
`SourceAddress`	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
`SourcePort`	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
`SourceUserName`	User name of the user that exported the resources.

SourceUserID	ID of the user that exported the resources.
DeviceCustomString5	ID of the tenant from which the resources were exported.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	ID of the resource that was exported.
DeviceCustomString6Label	resource ID
DeviceCustomString4	Version of the resource that was exported.
DeviceCustomString4Label	version

Rule is linked to the collector

Event field name	Field value
DeviceAction	link rule to collector
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
ExternalID	ID of the service to which the rule was linked.
Name	Name of the service to which the rule was linked.
DeviceFacility	Action (rule is linked).
DeviceCustomString1	ID of the rule.
DeviceCustomString1Label	rule ID
DeviceCustomString2	Name of the rule.
DeviceCustomString2Label	rule name
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Rule is unlinked from the collector

Event field name	Field value
DeviceAction	unlink rule from collector
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.

SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
ExternalID	ID of the service from which the rule was unlinked.
Name	Name of the service from which the rule was unlinked.
DeviceFacility	Action (rule is unlinked).
DeviceCustomString1	ID of the rule.
DeviceCustomString1Label	`rule ID`
DeviceCustomString2	Name of the rule.
DeviceCustomString2Label	`rule name`
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	`tenant name`

Rule is linked to the correlator

Event field name	Field value
DeviceAction	`link rule to correlator`
EventOutcome	`succeeded`
SourceTranslatedAddress	This field contains the value of the HTTP header `x-real-ip` or `x-forwarded-for`. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
ExternalID	ID of the service to which the rule was linked.
Name	Name of the service to which the rule was linked.
DeviceFacility	Action (rule is linked).
DeviceCustomString1	ID of the rule.
DeviceCustomString1Label	`rule ID`
DeviceCustomString2	Name of the rule.
DeviceCustomString2Label	`rule name`
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	`tenant name`

Rule is unlinked from the correlator

Event field name	Field value
DeviceAction	unlink rule from correlator
EventOutcome	succeeded
SourceTranslatedAddress	This field contains the value of the HTTP header x-real-ip or x-forwarded-for. If these headers are absent, the field will be empty.
SourceAddress	The address from which the user logged in. If the user logged in using a proxy server, the address of the proxy server is specified.
SourcePort	Port from which the user logged in. If the user logged in using a proxy server, the port of the proxy server is specified.
SourceUserName	User name of the user that modified the data.
SourceUserID	ID of the user that modified the data.
ExternalID	ID of the service from which the rule was unlinked.
Name	Name of the service from which the rule was unlinked.
DeviceFacility	Action (rule is unlinked).
DeviceCustomString1	ID of the rule.
DeviceCustomString1Label	rule ID
DeviceCustomString2	Name of the rule.
DeviceCustomString2Label	rule name
DeviceCustomString5	Tenant ID.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Tenant name.
DeviceCustomString6Label	tenant name

Filters

Filters allow you select events based on specified conditions. You can use filters for collectors, correlators, storage, correlation rules, enrichment rules, aggregation rules, destinations, response rules, and segmentation rules. The collector service uses filters to select events that you want to send to KUMA. Events that satisfy filter conditions are sent to Kaspersky SIEM for further processing.

You can use standalone filters or built-in filters that are stored in the service or resource in which they were created. For resources in input fields except the **Description** field, you can enable the display of control characters.

Names of resources used in the filter are automatically specified. Fields containing the names of linked resources cannot be edited. The names of shared resource categories are not displayed in the filter if you do not have the "Read shared resources" role. To view the list of resources for the selected operand inside the expression, press **Ctrl+Space**. This displays a list of resources.

To view filters:

in the web interface, go to the **Resources** → **Filters** section.

The filter table opens.

You can use the **Search** field to search for filters by their names. Regular expressions are used when searching for filters.

You can sort the table by name, last update time, or package name by clicking the sort icon ⌄ in the column header and selecting either **Ascending** or **Descending**.

The filter table contains the following columns:

- **Name** is a filter name.
- **Resource path** is the tenant that owns the filter.
- **Updated** is the date and time of the last update of a filter.
- **Created by** is the name of a user who created a filter.
- **Description** is optional information about the filter.
- **Tags** serve for filter searching. To search for filters, click the sort icon in the column header, and specify a value to search for in the **Search** field or select tags using check boxes.
- **Package name** is the name of the package of tools for event processing.

When creating a filter, you must specify the operands and operators. The available operator types depend on the selected left (L) or right (R) operands.

Available operator types for left (L) and right (R) operands

Operator	"Event fields" type	"Active lists" type	"Dictionaries" type	"Context tables" type	"Tables" type	TI type	"Constant" type	"List" type
=	L, R	L, R	L, R	L, R	L, R	L, R	R	R
>	L, R	L, R	L, R	L, R (only when looking up a table value by index)	L, R	L	R	—
>=	L, R	L, R	L, R	L, R (only when looking up a table value by index)	L, R	L	R	—
<	L, R	L, R	L, R	L, R (only when looking up a table value by index)	L, R	L	R	—
<=	L, R	L, R	L, R	L, R (only when looking up a table value by index)	L, R	L	R	—
insubnet	L, R	L, R	L, R	L, R	L, R	L, R	R	R
contains	L, R	L, R	L, R	L, R	L, R	L, R	R	R
startsWith	L, R	L, R	L, R	L, R	L, R	L, R	R	R
endsWith	L, R	L, R	L, R	L, R	L, R	L, R	R	R
match	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—

inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

Shortcut keys when working with filters

You can use hotkeys when managing filters (see the table below).

Hotkeys and their functions

Key	Function
`e`	Invokes a filter by the event field.
`d`	Invokes a filter by the dictionary field.
`a`	Invokes a filter by the active list field.
`c`	Invokes a filter by the context table field.
`t`	Invokes a filter by the table field.
`f`	Invokes a filter.
`t+i`	Invokes a filter using TI.
`Ctrl+Enter`	Finish editing a condition.

Filters with extended event schema

The usage of extended event schema fields of the `String`, `Number`, or **Float** types is the same as the usage of fields of the KUMA event schema.

When using filters with extended event schema fields of the `Array of strings`, `Array of integers`, and `Array of floats` types, you can use the following operators:

- **contains** returns `True` if the specified substring is present in the array, otherwise it returns `False`.
- **match** searches within a string using a regular expression.
- **intersec**.

Predefined filters

The filters listed in the table below are included in the KUMA kit.

Filter name	Description
[OOTB][AD] A member was added to a security-enabled global group (4728)	Selects events of adding a user to an Active Directory security-enabled global group.
[OOTB][AD] A member was added to a security-enabled universal group (4756)	Selects events of adding a user to an Active Directory security-enabled universal group.
[OOTB][AD] A member was removed from a security-enabled global group (4729)	Selects events of removing a user from an Active Directory security-enabled global group.
[OOTB][AD] A member was removed from a security-enabled universal group (4757)	Selects events of removing a user from an Active Directory security-enabled universal group.
[OOTB][AD] Account Created	Selects Windows user account creation events.
[OOTB][AD] Account Deleted	Selects Windows user account deletion events.
[OOTB][AD] An account failed to log on (4625)	Selects Windows login failure events.
[OOTB][AD] Successful Kerberos authentication (4624, 4768, 4769, 4770)	Selects successful Windows login events and events with IDs 4769 and 4770 that are logged on domain controllers.
[OOTB][AD][Technical] 4768. TGT Requested	Selects Microsoft Windows events with ID 4768.
[OOTB][Net] Possible port scan	Selects events that may indicate a port scan.
[OOTB][SSH] Accepted Password	Selects events of successful SSH connections with a password.
[OOTB][SSH] Failed Password	Selects attempts to connect over SSH with a password.

Sending test events to KUMA

KUMA allows sending test events to the system. Use the option of sending test events to KUMA to test rules, reports, dashboards, and also to check the resource consumption of the collector with different event streams. Events can only be sent to a collector that receives events over TCP or HTTP.

During the initial solution configuration, if you need to verify the collector configuration, you can send a single test event to the collector port. Instructions for this case are given in the section Port check.

To send test events, you need:

- The 'kuma' file started with certain options.

  In the following instructions, the file with raw events is named send_test_events.txt as an example. You can use your own file name.

- A configuration file in which you define the parameters for running the executable file.

  In the following instructions, the configuration file is named config_for_test_events as an example. You can use your own file name.

To send test events:

1. Get sample events to send to KUMA:

   a. In the KUMA web interface, in the **Events** section, in the upper right corner, click the ⚙ icon and in the displayed window, on the **Event fields columns** tab, select the check box for the **Raw** field. The 'Raw' column is displayed in the **Events** window.

   b. Search for events.

   c. Export your search results: in the **Events** window, in the upper right corner, click ... and select **Export TSV**.

d. Go to the **Task manager** section of KUMA and click the **Events export** task; in the context menu, select **Download**.

The `<name of file with exported events>`.tsv file is displayed in the Downloads section.

If you are not collecting raw events, enable collection for a short time by setting the **Keep raw event** setting of the normalizer to **Always**. After the collection is completed, restore the previous value of the **Keep raw event** setting.

e. Create a text file named send_test_events.txt and copy the contents of the `Raw` field from `<name of file with exported events>`.tsv to a text file named send_test_events.txt.

f. Save send_test_events.txt.

2. Create a config_for_test_events configuration file and add the following lines to the file:

```
{
"kind": "<tcp or http>",
"name": "-",
"connection": {
"name": "-",
"kind": "<tcp or http>",
"urls": ["< IP address of the KUMA collector for receiving events over TCP >:< port of the KUMA collector for receiving event over TCP >"]
}
}
```

Save the config_for_test_events configuration file.

3. Ensure that network connectivity exists between the server sending events and the server on which the collector is installed.

4. To send the contents of the test event file to the KUMA collector, run the following command:

```
/opt/kaspersky/kuma/kuma tools load --raw --events /home/events/send_test_events.txt --cfg home/events/config_for_test_events --limit 1500 --replay 100000
```

Available settings

Setting	Description
`--events`	Full path to the file containing raw events. Required setting. If the full path is not specified, the command does not run.
`--cfg`	Path to the configuration file. Required setting. If the full path is not specified, the command does not run.
`--limit`	Stream to be sent to the collector, in events per second (EPS). Required setting. If no value is specified, the command does not run.
`--replay`	Number of events to send. Required setting. If no value is specified, the command does not run. The step for --replay is 10000. The minimum value is 10000. --replay 16 sends 10000 events. --replay 16000 sends 20000 events.

As a result of running the command, test events are successfully sent to the KUMA collector. You can verify the arrival of test events by searching for related events in the KUMA web interface.

Time format

KUMA supports processing information passed to the fields of the event data model with the timestamp type (EndTime, StartTime, DeviceCustomDate1, etc) in the following formats:

- "May 8, 2009 5:57:51 PM".
- "oct 7, 1970".
- "oct 7, '70".
- "oct. 7, 1970".
- "oct. 7, 70".
- "Mon Jan 2 15:04:05 2006".
- "Mon Jan 2 15:04:05 MST 2006".
- "Mon Jan 02 15:04:05 -0700 2006".
- "Monday, 02-Jan-06 15:04:05 MST".
- "Mon, 02 Jan 2006 15:04:05 MST".
- "Tue, 11 Jul 2017 16:28:13 +0200 (CEST)".
- "Mon, 02 Jan 2006 15:04:05 -0700".
- "Mon 30 Sep 2018 09:09:09 PM UTC".
- "Mon Aug 10 15:44:11 UTC+0100 2015".
- "Thu, 4 Jan 2018 17:53:36 +0000".
- "Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)".
- "Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)".
- "September 17, 2012 10:09am".
- "September 17, 2012 at 10:09am PST-08".
- "September 17, 2012, 10:10:09".
- "October 7, 1970".
- "October 7th, 1970".
- "12 Feb 2006, 19:17".
- "12 Feb 2006 19:17".

- "14 May 2019 19:11:40.164".
- "7 oct 70".
- "7 oct 1970".
- "03 February 2013".
- "1 July 2013".
- "2013-Feb-03".

dd/Mon/yyyy format

- "06/Jan/2008:15:04:05 -0700".
- "06/Jan/2008 15:04:05 -0700".

mm/dd/yyyy format

- "3/31/2014".
- "03/31/2014".
- "08/21/71".
- "8/1/71".
- "4/8/2014 22:05".
- "04/08/2014 22:05".
- "4/8/14 22:05".
- "04/2/2014 03:00:51".
- "8/8/1965 12:00:00 AM".
- "8/8/1965 01:00:01 PM".
- "8/8/1965 01:00 PM".
- "8/8/1965 1:00 PM".
- "8/8/1965 12:00 AM".
- "4/02/2014 03:00:51".

- "03/19/2012 10:11:59".
- "03/19/2012 10:11:59.3186369".

yyyy/mm/dd format

- "2014/3/31".
- "2014/03/31".
- "2014/4/8 22:05".
- "2014/04/08 22:05".
- "2014/04/2 03:00:51".
- "2014/4/02 03:00:51".
- "2012/03/19 10:11:59".
- "2012/03/19 10:11:59.3186369".

yyyy:mm:dd format

- "2014:3:31".
- "2014:03:31".
- "2014:4:8 22:05".
- "2014:04:08 22:05".
- "2014:04:2 03:00:51".
- "2014:4:02 03:00:51".
- "2012:03:19 10:11:59".
- "2012:03:19 10:11:59.3186369".

Format containing Chinese characters

"2014年04月08日"

yyyy-mm-ddThh format

- "2006-01-02T15:04:05+0000".
- "2009-08-12T22:15:09-07:00".
- "2009-08-12T22:15:09".
- "2009-08-12T22:15:09.988".
- "2009-08-12T22:15:09Z".
- "2017-07-19T03:21:51:897+0100".
- "2019-05-29T08:41-04" without seconds, 2-character TZ.

yyyy-mm-dd hh:mm:ss format

- "2014-04-26 17:24:37.3186369".
- "2012-08-03 18:31:59.257000000".
- "2014-04-26 17:24:37.123".
- "2013-04-01 22:43".
- "2013-04-01 22:43:22".
- "2014-12-16 06:20:00 UTC".
- "2014-12-16 06:20:00 GMT".
- "2014-04-26 05:24:37 PM".
- "2014-04-26 13:13:43 +0800".
- "2014-04-26 13:13:43 +0800 +08".
- "2014-04-26 13:13:44 +09:00".
- "2012-08-03 18:31:59.257000000 +0000 UTC".
- "2015-09-30 18:48:56.35272715 +0000 UTC".
- "2015-02-18 00:12:00 +0000 GMT".
- "2015-02-18 00:12:00 +0000 UTC".
- "2015-02-08 03:02:00 +0300 MSK m=+0.000000001".

- "2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001".
- "2017-07-19 03:21:51+00:00".
- "2014-04-26".
- "2014-04".
- "2014".
- "2014-05-11 08:20:13,787".

yyyy-mm-dd-07:00 format

"2020-07-20+08:00"

mm.dd.yyyy format

- "3.31.2014".
- "03.31.2014".
- "08.21.71".

yyyy.mm.dd format

- "2014.03.30"

yyyymmdd format and similar

- "20140601".
- "20140722105203".

yymmdd hh:mm:yy format

"171113 14:14:20"

Unix timestamp format

- "1332151919".
- "1384216367189".
- "1384216367111222".
- "1384216367111222333".

Mapping fields of predefined normalizers

The file available via the download link contains a description of the field mapping of preset normalizers.

Download Description of field mapping of preset normalizers.

Deprecated resources

List of deprecated resources

Name	Resource type	Description
[Deprecated][OOTB] Microsoft SQL Server xml	Normalizer	This normalizer was removed from the resource set in KUMA 3.2. If you were using this normalizer, you must migrate to the [OOTB] Microsoft Products for KUMA 3 normalizer.
[Deprecated][OOTB] Windows Basic	Normalizer	This normalizer was removed from the resource set in KUMA 3.2. If you were using this normalizer, you must migrate to the [OOTB] Microsoft Products for KUMA 3 normalizer.
[Deprecated][OOTB] Windows Extended v.0.3	Normalizer	This normalizer was removed from the resource set in KUMA 3.2. If you were using this normalizer, you must migrate to the [OOTB] Microsoft Products for KUMA 3 normalizer.
[Deprecated][OOTB] Cisco ASA Extended v 0.1	Normalizer	This normalizer was removed from the resource set in KUMA 3.2. If you were using this normalizer, you must migrate to the [OOTB] Cisco ASA and IOS syslog normalizer.
[Deprecated][OOTB] Cisco Basic	Normalizer	This normalizer was removed from the resource set in KUMA 3.2. If you were using this normalizer, you must migrate to the [OOTB] Cisco ASA and IOS syslog normalizer.
[Deprecated][OOTB] Linux audit and iptables syslog	Normalizer	This normalizer was removed from the resource set in KUMA 3.4. In KUMA 3.2, we recommend using the [OOTB] Linux auditd syslog for KUMA 3.2 normalizer.
[Deprecated][OOTB] Linux audit.log file	Normalizer	This normalizer was removed from the resource set in KUMA 3.4. In KUMA 3.2, we recommend using the [OOTB] Linux auditd file for KUMA 3.2 normalizer.
[OOTB] Checkpoint Syslog CEF by CheckPoint	Normalizer	This normalizer was removed from the resource set in KUMA 3.4. In KUMA 3.4 and newer versions, we recommend using the [OOTB] Checkpoint syslog normalizer.
[OOTB] Eltex MES Switches	Normalizer	This normalizer was removed from the resource set in KUMA 3.4. In KUMA 3.4 and newer versions, we recommend using the [OOTB] Eltex MES syslog, [OOTB] Eltex ESR syslog normalizers.

Name	Resource type	Description
[OOTB] PTsecurity NAD	Normalizer	This normalizer was removed from the resource set in KUMA 3.4. In KUMA 3.4 and newer versions, we recommend using the [OOTB] PTsecurity NAD json normalizer.
[OOTB][AD] Granted TGS without TGT (Golden Ticket)	Rule	The rule was removed from the KUMA 3.4 resource set.
[OOTB][AD] Possible Kerberoasting attack	Rule	The rule was removed from the KUMA 3.4 resource set.
[OOTB][AD][Technical] 4768. TGT Requested	Rule	The rule was removed from the KUMA 3.4 resource set.
[OOTB][AD] List of requested TGT. EventID 4768	Active list	The list was removed from the KUMA 3.4 resource set.
[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	Normalizer	This normalizer is obsolete and was removed from the KUMA 4.6 resource set. We recommend using the [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog normalizer.
[OOTB] VipNet Coordinator Syslog Direction	Dictionary	The [OOTB] VipNet Coordinator Syslog Direction dictionary is obsolete and was removed from the KUMA 4.6 resource set.

Generating events for testing a normalizer

If necessary, you can generate your own example events to test your normalizer. Such testing makes it easier to write regular expressions and lets you see which values end up in the KUMA event fields.

Keep in mind the following special considerations:

- This tests simulates event processing. Example events in the **Example event** field are intended for displaying examples in the **Field mapping** section. Examples of the parent normalizer are used to generate examples of child normalizers, taking into account the **Field to pass into normalizer** setting.
- Mutations cannot be applied.

To test the normalizer, you need to add an example event to the **Event examples** field in the selected normalizer and start generating events by using the relevant command. As a result of running the command, KUMA takes the example event from the **Example event** field and sends events to the normalizer with the specified interval. If necessary, you can specify multiple examples to get events for multiple examples.

To test the normalizer:

1. Select the collector that you want to use for testing:
   - If the collector is installed on the server and running, stop the collector service:

     ```
     sudo systemctl stop kuma-collector-<service_ID>.service
     ```

     where:

     <service_ID> is the service ID copied from the KUMA web interface.
   - If the collector is not running, or is in the process of being created or edited, proceed to the next step.

2. In the collector creation wizard, if necessary, fill in or edit the required fields at the **Connect event sources** step and at the **Transport** step, then proceed to the **Parsing** step:

   a. Link a normalizer by selecting it from the drop-down list, or create a normalizer.

   b. In the **Event examples** field, add example events. For example, for a json normalizer, you can add the following value: `{"name": "test_events", "address": "10.12.12.31"}`. You can specify multiple examples if you want to receive events for multiple examples in the same normalizer. Events are generated for each example.

3. In the Collector Installation Wizard, go to the **Routing** step and specify the storage where you want to save test events.

4. Review the collector settings and click **Save**.

5. Go to the **Active services** section in KUMA and click **Add** to add a collector. This opens the **Choose a service** window; in that window, select the collector and click **Create service**. The collector is displayed in the **Active services** list.

6. Check the status of the collector to which events are being sent. The collector status should be red.

7. Run the event generation command with the necessary parameters:

   - If the collector is not installed on the server, but only added in the **Active services** section:

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <CA_cert_ID> --
     generator.interval <interval> --id <service_ID> --api.port <API_port>
     ```

     where:

     - <FQDN> is the fully qualified domain name of the KUMA Core server.

     - <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).

     - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

       The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
       You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

       To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.

     - <interval> is the interval in seconds for generating and sending events. If the value of the event generation and sending interval is not specified or it is set to zero, events are not generated.

     - <service_ID> is the collector ID copied from the KUMA web interface.

     - <API_port> is the number of a free, unused API port.

- If the collector is installed on the server:

  ```
  sudo /opt/kaspersky/kuma/kuma collector --generator.interval <interval> --pair.fingerprint <CA_cert_ID> --
  id <service_ID> --api.port <API_port>
  ```

  where:

  - <interval> is the interval in seconds for generating and sending events. If the value of the event generation and sending interval is not specified or it is set to zero, events are not generated.
  - <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

    The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
    You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

    To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
  - <service_ID> is the collector ID copied from the KUMA web interface.
  - <API_port> is the number of a free, unused API port.

  As a result, KUMA generates events and sends them to the normalizer, observing the specified interval.

  You can verify that events have been created and satisfy your expectations in the **Events** section. For details about the check, you can refer to the `/etc/systemd/system/multi-user.target.wants/kuma-collector-<service_ID>.service` file.

If the result does not meet expectations, modify the example event:

- If the collector is not installed on the server and has only been in the **Active services** section, edit the **Event examples** field in the normalizer of the collector and save the collector settings.
- If the collector is installed on the server and stopped as a service, edit the **Event examples** field in the normalizer of the collector, save the collector settings, go to the **Active services** section, select the collector, and refresh the collector settings by clicking **Refresh**.

If the result meets expectations:

1. Disable event generation, for example, by pressing **`Ctrl+C`** on the command line.
2. Start the collector service; if the service is already installed on the server, but has been stopped:

   ```
   sudo systemctl start kuma-collector-<service_ID>.service
   ```

   where:

   <service_ID> is the collector ID copied from the KUMA web interface.

3. If the collector has only been added in the **Active services** section, but has not been installed on the server yet, install the collector on the server using the following command:

```
sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID>
--api.port <API_port> --install
```

where:

- <FQDN> is the fully qualified domain name of the KUMA Core server.
- <port> is the port that KUMA Core uses for internal communications (port 7210 is used by default).
- <CA_cert_ID> is the fingerprint ID of the CA certificate used for authentication when connecting the service.

  The `--pair.fingerprint` argument is optional. When creating a service, KUMA automatically adds this option to the installation command and specifies the fingerprint ID.
  You can install a service without specifying the `--pair.fingerprint` option. In this case, KUMA uses an `insecure` value by default, which skips the validation of the KUMA Core CA certificate when establishing a connection. If set to is `insecure`, the fingerprint does not need to be updated after the CA certificate is reissued.

  To make sure the KUMA Core CA certificate gets validated, we recommend keeping the `--pair.fingerprint` option with the fingerprint ID when installing the service. When reissuing a CA certificate, you need to copy the new certificate fingerprint from the web interface and restart the service with the updated fingerprint ID.
- <service_ID> is the collector ID copied from the KUMA web interface.
- <API_port> is the port used for communication with the component being installed.

Legal information

This section contains legal information.

Licensing

A *License* is a time-limited right to use KUMA, granted to you under the terms of the End User License Agreement. The scope of services and the duration of usage depend on the type of license under which the solution is being used.

A license is provided when the application is purchased. If there is no license:

- After the expiration of the license, KUMA keeps working for 7 days without restrictions on functionality, that is, collectors continue to receive and process events. After 7 days pass, the collectors and correlators restart and stop accepting and processing new events. The rest of the running services continue to work. Events saved before the reception is stopped are not deleted and remain available for searching and viewing during the configured retention period.

- If the license key is removed, KUMA collectors immediately stop receiving and processing new events. Old events remain available.

- Creating and editing resources, creating and running services becomes impossible.

Activating the solution

To activate and then use KUMA in accordance with the terms and conditions of the End User License Agreement, you must add a *license key*, which is a unique sequence of bits, to the solution. License keys are generated by Kaspersky specialists.

When you purchase the solution, you get two license keys. One license key allows you to activate KUMA. The second key allows Kaspersky Endpoint Security to send operating system events to KUMA collectors.

You can add a license key by using an *activation code* or *key file* provided to you after purchasing the license.

About the key file

Key file is a file with the key extension provided to you by Kaspersky. The key file is used to add a license key that activates the solution.

You receive a key file at the email address that you provided after purchasing KUMA.

You do not need to connect to Kaspersky activation servers in order to activate the solution with a key file.

If the key file has been accidentally deleted, you can restore it. You may need a key file, for example, to register with Kaspersky CompanyAccount.

To restore the key file, you need to do one of the following:

- Contact the license seller.
- Get a key file on the Kaspersky website based on the available activation code.

About the activation code

An *activation code* is a unique sequence of twenty Latin letters and numerals. You enter an activation code to add a license key that activates KUMA. The key file is sent to the email address that you specified after purchasing KUMA.

To activate the solution using the activation code, the KUMA Core server needs internet access to connect to the Kaspersky activation server at the following address:

```
https://activation-v2.kaspersky.com:443
```

In the case of a closed infrastructure, you can specify a proxy server.

If the activation code has been lost after activating KUMA, contact the Kaspersky partner from which you purchased the license.

If you have activated the solution using a key file before and are renewing the license by using an activation code, the activation is performed seamlessly if the parameters of the activation code fully match the parameters of the key file. If there are any differences in the parameters, the services are restarted.

> When switching from a key file to an activation code, the previously added license key is automatically deleted. Before renewing the license, make sure that you have the old key file on hand.

When adding or removing a license key, as well as when the license expires, KUMA generates an audit event.

You can add a license key in the following ways:

- During the installation of KUMA.
- In the **License** section of the web interface of the solution.

The license key is displayed in the web interface of the solution as a unique alphanumeric sequence after you add it to the solution.

The license key may be blocked by Kaspersky in case the terms of the License Agreement have been violated. If the license key has been blocked, you need to add another one if you want to use the solution.

The license key that is currently being used by solution becomes the *active license key*. The solution cannot have more than one active license key.

Renewing the license

We recommend that you renew your license no later than its expiration date to ensure maximum protection against cyberthreats.

To ensure timely renewal of the license, you can add a reserve license key in advance.

A *reserve license key* is the license key that entitles the user to use KUMA, but is not currently in use. A backup license key automatically becomes active when the license associated with the current active license key expires. A backup license key can be added only if an active license key is present. A trial license key cannot be used as a backup license key.

About the License Certificate

Along with the key file or activation code, you also receive a *License Certificate*, which contains the following information about the provided license:

- License ID or order number
- Information about the user who is granted the license
- Information about the solution that can be activated under the provided license
- Restriction on the number of licensing units (for example, the number of events that can be processed per second)
- Start date of the license term
- License expiration date or license term
- License type

Viewing the End User License Agreement

The *End User License agreement* is a legal agreement between you and AO Kaspersky Lab that specifies the conditions under which you can use the solution.

Read the terms of the End User License Agreement carefully before using the solution for the first time.

You can familiarize yourself with the terms of the End User License Agreement in the following ways:

- Go to the directory with the extracted installer and read the `./roles/kuma/files/LICENSE` text file.
- Go to the directory with the extracted installer and run the following command to display the text of the End User License Agreement:

  ```
  ./roles/kuma/files/kuma license --show
  ```

- On a host with any KUMA component installed (such as KUMA Core, collector, correlator, storage), run the following command to display the text of the End User License Agreement:

  ```
  /opt/kaspersky/kuma/kuma license --show
  ```

- On devices included in the `kuma_storage`, `kuma_collector`, `kuma_correlator`, or `kuma_core` sections in the inventory file, open the `LICENSE` file in the `/opt/kaspersky/kuma` directory.

  On a host in the kuma_core group, you can view the End User License Agreement only if a non-cluster installation is selected.

- On the Windows agent, run the following command to display the text of the End User License Agreement:

  ```
  .\kuma.exe license --show
  ```

- On the Linux agent, go to the directory with the 'agent' executable file and run the following command to display the text of the End User License Agreement:

  ```
  ./agent license --show
  ```

You accept the terms of the End User License Agreement by confirming your acceptance of the End User License Agreement during the solution installation. If you do not accept the terms of the End User License Agreement, you must cease the installation of the solution and must not use the solution.

License groups and merged license

License groups

You can a license key in the KUMA web interface If you use a key file to activate the solution, there can be two license keys: an active key and a reserve key. If you use an activation code, there is only one license key. In KUMA, a group of an active and a reserve license keys or one activation code is called a *license group*. Accordingly, you can add a license group using two key files or using an activation code.

Merged license

If multiple license groups are added to an instance of KUMA, the active license keys of all license groups are automatically merged. This creates a *merged license*. License keys of such a license are merged in accordance with the following rules:

- The **EPS available** values of all active license keys are added together. The resulting EPS value is specified in the merged license and becomes available to all tenants.

  If any license key included in the merged license expires, the EPS limit value of that license key is automatically subtracted from the total EPS limit of the merged license. Accordingly, when a new active license key is added to the merged license, the EPS limit value of that license key is automatically added to the total EPS limit.

- The set of modules available in tenant licenses must be the same. If a license contains a module that is not available in the other licenses, this module is not available in the merged license. Accordingly, such a module is not available to any of the tenants.

  The same rule applies when adding new license keys to the merged license. If a module is available in the new license key, but is not available in the merged license, this module does not become available under the merged license. If a module that is available in the merged license is not available in the new license key, this module will become unavailable under the merged license. When adding a license key with a mismatched set of modules, KUMA displays a warning and adds this license key only after your confirmation.

- A merged license can include up to 50 active keys.

Example of using a merged license

This example shows the use of a merged license in a holding combining companies A, B, and C. One shared instance of KUMA is deployed in the holding, and multi-tenancy is configured.

Companies A, B, and C must each subsequently purchase a license of their own to use the solution.

To solve this problem, use a merged license:

1. Each of the companies A, B, and C acquires a KUMA license in the form of a license certificate and a key file or activation code, and transfers the received key files or activation codes to the KUMA General Administrator.

2. KUMA General Administrator adds three active license keys in the KUMA web interface.

   The added license keys are automatically merged with the license keys that activated the solution during deployment. As a result, a merged license is created, the details of which are displayed in the **Settings** → **Other** → **License** section above the table of license groups.

Managing license keys in the KUMA web interface

This article describes how to view information about license keys, how EPS is calculated, how to add and delete a license key, replace an active license key, and add a reserve license key to a license group.

Viewing information about license keys

To view information about license keys, you need Manage or Read rights to the License functional area. Among the predefined roles, only the General Administrator has this permission.

To view information about the added license keys:

In the KUMA web interface, open the **Settings** → **Other** → **License** section.

It displays the following information:

- **License key name**—contains the name of a solution and additional parameters, if applicable.
- Unique alphanumeric sequence of the license key.
- **EPS available** is the number of events processed per second supported by the license.
- **EPS current per day current per day** is the current average events per second number as calculated from the events processed during the available observation period of up to 24 hours.
- **EPS current per hour** is the current average events per second processed in the last hour. This figure is available only for SMART I and SMART II licenses.
- **Expiration date** is the date when the license key will expire.
- **Remaining** is the number of days before the license expires.
- **Modules** are modules covered by the license.

EPS calculation

Only normalized events are taken into account when calculating the EPS. Events are counted at the output of the collector after processing operations, including filtering, aggregation, and enrichment have been completed. If one event is dispatched to multiple destinations after being processed by the collector, it is counted as one event.

The **EPS current per day** value is calculated for all licenses. This figure is calculated based on the number of events processed by collectors over the available observation period of up to 24 hours. The following formula is used for the calculation:

```
(x1 + x2 + ... + xn) / (m × 3600) = EPS
```

where:

`x1, x2, ... xn` is the number of events processed by each collector over the available observation period.

`n` is the number of collectors.

`m` is the number of available hour-long windows.

`3600` is the number of seconds in an hour.

The number of available hour-long windows can be less than 24 if, for example, the collectors were started less than 24 hours ago. In this case, the calculation is performed for the hour-long windows that are actually available. For example, if the collectors have been running for three hours, three hour-long windows are used for the calculation.

For SMART I and SMART II licenses, the **EPS current per hour** is additionally calculated. It is calculated from the number of events processed by all collectors over the last hour, using the following formula:

```
(x1 + x2 + ... + xn) / 3600 = EPS
```

where:

`x1, x2, ... xn` is the number of events processed by each collector over the last hour.

`n` is the number of collectors.

`3600` is the number of seconds in an hour.

Exceeding the EPS limit

The EPS should be monitored by looking at figures displayed in the license key details:

- **EPS current per day** for all licenses
- **EPS current per hour** for SMART I and SMART II licenses.

If the calculated EPS exceeds the EPS specified in the license, KUMA displays information about the EPS being exceeded in the **Events** section.

For licenses with an EPS limit at the tenant level, when this limit is exceeded, KUMA also displays information about the limit being exceeded in the **Events** section. A value of 0 means that no limit is set.

For SMART I and SMART II licenses, when **EPS current per day** and **EPS current per hour** limits are exceeded simultaneously, the collector with the maximum EPS stops receiving new events for one hour. Multiple collectors may be paused at the same time. A notification about the maximum EPS allowed by the license being exceeded is sent to a user with the General administrator role. A collector with an imposed restriction continues to receive events, but does not process the events until the restriction is lifted. On the active services page, such a collector is displayed with a red status.

After one hour, the collector resumes operation.

Adding a license key

To add a license key:

1. In the KUMA web interface, open the **Settings** → **Other** → **License** section.

   The table of the added license groups opens.

2. Click **Add license key**.

3. This opens a window; in that window, enter a name for the license group.

4. Then click the **Add** button.

   The new license group will be displayed in the table.

   You can rename a group of licenses. To do this, check the box next to the required group of licenses, click **Rename**, in the window that opens, specify a new name for the group, and save the changes.

5. Click the name of the added license group.

   This opens the license group configuration window.

6. Select the method for adding the license key:

   - Using an activation code:

     a. Enter the activation code.

     b. If your company uses a proxy server to connect to the internet, enter proxy server information. An internet connection is required to activate the solution.

   - Using a key file:

     a. In the **Active license key** section, click the **Upload** button, then select the key file (the one with KEY extension).

     b. In the **Reserve license key** section, add the backup license key in the same way.

7. Then click the **Add** button.

   The license key is added.

Deleting a license key

In KUMA, you can remove an added license key from the program (for example, if you need to replace the current license key with a different one). After the license key is removed, collectors immediately stop receiving and processing events. Old events remain available. Creating and modifying resources, creating and running services also becomes impossible. This functionality will be re-activated after you add a license key.

> To delete license keys, you need the Manage right to the License functional area. Among the predefined roles, only the General Administrator has this permission.

To delete an added license key:

1. In the KUMA web interface, open the **Settings** → **Other** → **License** section.

   The table of the added license groups opens.

2. Select the check box next to the license group that contains the license key that you want to delete.

3. Click the **Delete** button.

   A confirmation window opens.

4. Confirm the deletion of the license group.

   The license key will be deleted.

Replacing the active license key

To replace an active license key:

1. Delete the current license key (see instructions above).
2. Add a new license key (see instructions above).

Adding a reserve license key to a license group

To add a reserve license key to a license group:

1. In the KUMA web interface, open the **Settings** → **Other** → **License** section.
   The table of the added license groups opens.
2. Click the name of the license group to which you want to add the reserve license key.
3. In the window that opens, in the **Reserve license key** section, click the **Upload** button, then select the key file (the one with KEY extension).
4. Then click the **Add** button.

Data provision

Data provided to third parties

KUMA functionality does not involve automatic provision of user data to third parties.

Locally processed data

Kaspersky Unified Monitoring and Analysis Platform (hereinafter KUMA or "program") is an integrated software solution that includes the following primary functions:

- Receiving, processing, and storing information security events
- Analyzing and correlating incoming data
- Searching in received events
- Creation of notifications upon detecting symptoms of information security threats.
- Creation of alerts and incidents for processing information security threats.

- Displaying information about the status of the customer's infrastructure on the dashboard and in reports.
- Monitoring event sources.
- Device (asset) management—viewing information about assets, searching, adding, editing, and deleting assets, exporting asset information to a CSV file.

To perform its primary functions, KUMA may receive, store and process the following information:

- Information about devices on the corporate network.

  The KUMA Core server receives data if the corresponding integration is configured. You can add assets to KUMA in the following ways:

  - Import assets:
    - On demand from MaxPatrol.
    - On a schedule from Kaspersky Security Center and KICS/KATA.
  - Create assets manually through the web interface or via the API.

  KUMA stores the following device information:

  - Technical characteristics of the device.
  - Vulnerabilities of the asset.
  - Information specific to the source of the asset.
- Additional technical attributes of devices on the corporate network that the user specifies to send an incident to NCIRCC: IP addresses, domain names, URIs, email address of the attacked object, attacked network service, and port/protocol.
- Data received from GosSOPKA and messages from NCIRCC: information about the organization of the GosSOPKA subject, category and type of event, technical information about the malicious system (including domain name, IP addresses, hash, URI, email address), information about vulnerabilities of the attacked application and information about the attacked object.
- Information about the organization: name, tax ID, address, email address for sending notifications.
- Active Directory information about organizational units, domains, users, and groups obtained as a result of querying the Active Directory network.

  The KUMA Core server receives this information if the corresponding integration is configured. To ensure the security of the connection to the LDAP server, the user must enter the server URL, the Base DN, connection credentials, and certificate in the KUMA console.
- Information contained in events from configured sources.

  In the collector, the event source is configured, KUMA events are generated and sent to other KUMA services. Sometimes events can arrive first at the agent service, which relays events from the source to the collector. Additionally, you can configure the saving of the address or host name of the event aggregator server.

- Information required for the integration of KUMA with other applications (Kaspersky Threat Lookup, Kaspersky CyberTrace, Kaspersky Security Center, Kaspersky Industrial CyberSecurity for Networks, Kaspersky Automated Security Awareness Platform, Kaspersky Endpoint Detection and Response, Security Orchestration, Automation and Response SOAR, AI services: AI score and asset status, Kaspersky Investigation & Response Assistant).

  It can include certificates, tokens, URLs or credentials for establishing a connection with the other application, or other data necessary for the basic functionality of KUMA, for example, an email address. The user enters this data in the KUMA console

- Information about sources from which event receipt is configured.

  It can include the source name, host name, IP address, the monitoring policy assigned to the source. The monitoring policy specifies the email address of the person responsible, to whom a notification will be sent if the policy is violated.

- User accounts: name, username, email address. The user can view their profile data in the KUMA console.

- User profile settings:

  - User role in KUMA. Assigned roles will be displayed.

  - Localization language, notification settings, display of non-printable characters.

    The user enters this data in the KUMA interface.

  - List of asset categories in the **Assets** section, default dashboard, TV mode flag for the dashboard, SQL query for default events, default preset.

    The user specifies these settings in the corresponding sections of the KUMA console.

- Data for domain authentication of users in KUMA:

  - Active Directory: root DN for searching access groups in the Active Directory directory service, URL of the domain controller, certificate (the root public key that the AD certificate is signed with), full path to the access group of users in AD (distinguished name).

  - Active Directory Federation Services: trusted party ID (KUMA ID in AD FS), URI for getting Connect metadata, URL for redirection from AD FS, and the AD FS server certificate.

  - FreeIPA: Base DN, URL, certificate (the public root key that was used to signed the FreeIPA certificate), custom integration credentials, connection credentials.

- Audit events

  KUMA automatically records audit events.

- KUMA log

  The user can enable extended logging in the KUMA console. Log entries are stored on the user's device, no data is transmitted automatically.

- Information about the user accepting the terms and conditions of legal agreements with Kaspersky.

- Information about current licenses in KUMA.

- Any information that the user enters in the KUMA interface.

The information listed above can find its way into KUMA in the following ways:

- The user enters information in the KUMA console.
- KUMA services (agent or collector) receive data if the user has configured a connection to event sources.
- Through the KUMA REST API.
- Device information can be obtained using the utility from MaxPatrol.

The listed information is stored in the KUMA database (ClickHouse, SQLite). Passwords are stored in an encrypted form (the hash of the password is stored).

All of the information listed above can be transmitted to Kaspersky only in dump files, trace files, or log files of KUMA components, including log files created by the installer and utilities.

Dump files, trace files, and log files of KUMA components may contain personal and confidential information. Dump files, trace files, and log files are stored on the device in unencrypted form. Dump files, trace files, and log files are not automatically submitted to Kaspersky, but the administrator can manually submit this information to Kaspersky at the request of Technical Support to help troubleshoot KUMA problems.

Kaspersky uses the collected data in anonymized form and only for general statistical purposes. Summary statistics is generated from the received raw data automatically and does not contain any personal or other confidential information. When new data accumulates, older data is erased (once a year). Summary statistics is stored indefinitely.

Kaspersky protects all received data in accordance with applicable law and Kaspersky policies. Data is transmitted over secure communication channels.

Compliance with European Union legislation (GDPR)

Regardless of the type of information and the territory from which it was received, Kaspersky adheres to high standards of data protection and employs legal, organizational, and technical measures to protect user data, guarantee security and confidentiality, and ensure the realization of user rights as guaranteed by applicable law.

Before using KUMA, read the description of data that is transferred. If your local law or standard may construe data transfered out of KUMA as personal data, you must take steps to ensure the legality of processing such data and obtain end users' consent to collection and transfer of such data.

In KUMA, compliance with European Union legislation (GDPR) is ensured by using the `log_archive_setup.py` tool. This tool lets you to install a worker script and a cron job to perform the following sequence of operations with log files:

1. Archival
2. Hashing
3. Encryption
4. Check
5. Deletion of cleartext data
6. Agent restart

Files are written to the `/etc/cron.d/` and `/usr/local/sbin/` directories.

Data integrity is ensured as follows:

- At the event level, by SHA256-hashing each raw line of the log file. The data is stored inside the archive.
- At the archive level, by SHA256-hashing the file with the .gpg extension. Data is stored as a file with the .sha256 extension next to the archive.

Data confidentiality is ensured by asymmetric GPG encryption, which makes sure that only the owner of the private key can decrypt the data.

Installing the log_archive_setup.py tool

By following this scenario, you can install and configure the worker script and the cron job.

1 Running the log_archive_setup.py tool

To run the `log_archive_setup.py` tool, you need root privileges on the KUMA agent host.

To run the `log_archive_setup.py` tool, run the following command:

```
sudo python3 log_archive_setup.py
```

If necessary, you can use the `--dry-run` flag to preview the objects being installed without writing any files. For this purpose, execute the following command:

```
sudo python3 log_archive_setup.py --dry-run
```

2 Selecting a target agent

To select a target agent, you need to specify its ID when specifying the agent name in the `kuma-agent-<id>.service` format.

Example

```
Enter %id% for kuma-agent-%id%: 001
```

The tool checks for the presence in systemd of the agent service that you specified. If this agent is not found, a list of all available `kuma-agent-*` services is displayed and the tool exits.

3 Creating an archival schedule

To create an archival schedule, set the following parameters:

- Archival frequency (1 to 7 days a week).
- Days of the week when archival is performed (1 stands for Monday and 7 for Sunday).
- The start time of the archival process in the HH:MM format. The default setting is 02:10.

After you set these parameters, the tool generates a cron expression, displays information for preview, and repeats its prompt you until you confirm.

Example

```
How many times per week? (1-7): 7
Enter time (HH:MM, 00:00..23:59) [02:10]: 03:00
Schedule preview:
  - Mode:   daily
  - Time:   03:00
  - Cron:   0 3 * * *
Apply this schedule? [y/N]: y
```

4 Looking up the recipient's GPG key

The `log_archive_setup.py` tool looks for an existing key in the following order:

- If the `/root/log-archive-keys/recipient_fingerprint.txt` fingerprint file exists and the public key is present in the protected database, the tool suggests reusing it.
- If the key with the user ID (UID) `log-archive@local` is present in the protected database, the tool suggests reusing it.
- If a key is not found, the tool generates a certificate and a 4096-bit RSA signature key in the isolated temporary GNUPGHOME directory. The following actions are performed:
  - the public and private keys are exported to the `/root/log-archive-keys` directory
  - The public key is imported into the protected database
  - A full encryption-decryption test of the keys is carried out.

5 Installing the worker script and the cron job

The worker script is written to the `/usr/local/sbin/log_archive_encrypt_<id>.py` directory with an embedded fingerprint of the GPG key and the name of the target application. The cron file is placed in the `/etc/cron.d/log-archive-encrypt-<id>` directory, and information about it is sent to the `/var/log/siem/archive/cron_<id>.log`.

After installing the worker script, encryption is automatically tested to verify that the tool works correctly.

For each file with the .log extension in the `/var/log/siem` directory, the worker script performs the following actions:

- Hashing the file line by line: reads a line of the file, calculates the SHA256 hash for that line and writes an auxiliary file with the .sha256 extension.
- Packaging: places the log file and the auxiliary file with the .sha256 extension into a .tar.gz archive with a timestamp (using atomic temporary files).
- GPG encryption: encrypts the .tar.gz archive using the recipient's fingerprint file.
- Determining the checksum of the archive: calculates the SHA256 hash of the entire file with the .gpg extension and writes it in the format <archive>.tar.gz.gpg.sha256 format.
- Renames temporary files to their final names, deletes the temporary .tar.gz archive, the auxiliary file with the .sha256 extension, and the original cleartext log file with the .log extension.
- Notifies the user about the need to move the `recipient_seckey.asc` secret key from the `/root/log-archive-keys/` directory to the security analyst's workstation and delete it from the agent host in accordance with the key management policy.
- Restarts the SIEM agent using the following command:

  ```
  systemctl try-restart kuma-agent-<id>.service
  ```

You can run the script with the following options:

- `--no-restart`: this option lets you skip the `systemctl try-restart` step.
- `--test-file <path>`: this option lets you process a specific file instead of all files with the .log extension.

When using the `log_archive_setup.py` tool, keep in mind the following:

- The archive directory is created in such a way that all output files are accessible only to the owner.
- For GPG encryption, the `--trust-model always` parameter is used, which is appropriate for a controlled key.

  > We do not recommend using this parameter with arbitrary keys from the outside.

- Cleartext from .log files is deleted only after the encrypted archive and its checksum have been successfully written.
- The `recipient_seckey.asc` private key is written to the `/root/log-archive-keys/` directory with only the owner having read and write permissions.

  > We recommend moving the private key to the workstation and deleting it from the agent host in accordance with the key management policy.

File and directory structure

The table below shows the structure of directories and files that the `log_archive_setup.py` tool uses, and the worker script.

Structure of directories and files

Directory or file	Description
`/var/log/siem`	Input files with the .log extension
`/var/log/siem/archive/<name>_<YYYY-MM-DD_HH-MM-SS>.tar.gz.gpg`	Encrypted archive
`/var/log/siem/archive/<name>_<YYYY-MM-DD_HH-MM-SS>.tar.gz.gpg.sha256`	Archive checksum
`/var/log/siem/archive/cron_<id>.log`	cron job log
`/usr/local/sbin/log_archive_encrypt_<id>.py`	Worker script
`/etc/cron.d/log-archive-encrypt-<id>`	cron job
`/root/log-archive-keys/recipient_fingerprint.txt`	Fingerprint of the GPG key
`/root/log-archive-keys/recipient_pubkey.asc`	Public key being exported
`/root/log-archive-keys/recipient_seckey.asc`	Private key

Deleting the worker script and the cron job

To delete the worker script and the cron job:

1. Do one of the following:

   - Run the following commands:

     ```
     rm /etc/cron.d/log-archive-encrypt-001
     rm /usr/local/sbin/log_archive_encrypt_001.py
     ```

     Where `001` is the agent ID.

   - Delete the GPG key from the protected database by running the following command:

     ```
     gpg --delete-key log-archive@local
     ```

2. If necessary, manually delete the archive files in the `/var/log/siem/archive/` directory and keys in the `/root/log-archive-keys/` directory.

Information about third-party code

Information about third-party code is in the LEGAL_NOTICES file located in the /opt/kaspersky/kuma/LEGAL_NOTICES folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

AMD is a trademark or registered trademark of Advanced Micro Devices, Inc.

Apache, Apache Cassandra, Apache Tomcat are either registered trademarks or trademarks of the Apache Software Foundation in the United States and/or other countries.

Ubuntu, LTS are registered trademarks of Canonical Ltd.

Cisco, IOS, Snort are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Citrix, Citrix NetScaler are either a registered trademark or a trademark of Cloud Software Group, Inc., and/or its subsidiaries in the United States and/or other countries.

Dameware, SolarWinds are trademarks that are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries.

Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc or its subsidiaries.

The Grafana word mark and the Grafana logo are either registered trademarks/service marks or trademarks/service marks of Coding Instinct AB, in the United States and other countries and are used with Coding Instinct's permission. We are not affiliated with, endorsed or sponsored by Coding Instinct, or the Grafana community. We are not affiliated with, endorsed, or sponsored by Coding Instinct, or the Grafana community.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.

ESET is trademark or registered trademark of ESET spol. s r.o. or respective ESET entity.

F5 is a trademark of F5 Networks, Inc. in the U.S. and in certain other countries.

Firebird is a registered trademark of the Firebird Foundation.

Fortinet, FortiGate, FortiMail, FortiOS, FortiSOAR are either registered trademarks or trademarks of Fortinet, Inc. in the United States and/or other countries.

The FreeBSD mark is a registered trademark of The FreeBSD Foundation.

Google, Chrome, Google Chrome are trademarks of Google LLC.

HUAWEI, Huawei Eudemon are trademarks of Huawei Technologies Co., Ltd.

IBM, Guardium, InfoSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Intel, Core are trademarks of Intel Corporation or its subsidiaries.

Juniper Networks and JUNOS are trademarks or registered trademarks of Juniper Networks, Inc. in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mac is a trademark of Apple Inc.

Microsoft, Active Directory, AppLocker, Azure, Excel, Halo, Hyper-V, Lync, Office 365, Outlook, PowerShell, SharePoint, Skype, SQL Server, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the U.S. and other countries.

NetApp is a trademark or registered trademark of NetApp, Inc. in the United States and/or other countries.

Netskope, the Netskope logo, and other Netskope product names referenced herein are trademarks of Netskope, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

OpenSSL is a trademark owned by the OpenSSL Software Foundation.

OpenVPN is a registered trademark of OpenVPN, Inc.

Oracle is a registered trademark of Oracle and/or its affiliates.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Ansible is a registered trademark of Red Hat, Inc. in the United States and other countries.

Sendmail, and other product designations or names are trademarks or registered trademarks of Sendmail, Inc.

Debian is a registered trademark of Software in the Public Interest, Inc.

The CommuniGate Pro name is a trademark or registered trademark of Stalker Software, Inc.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

OpenAPI is a trademark of The Linux Foundation.

Kubernetes is a registered trademark of The Linux Foundation in the United States and other countries.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

Trend Micro is a trademark or registered trademark of Trend Micro Incorporated.

The names, images, logos and pictures identifying UserGate's products and services are proprietary marks of UserGate and/or its subsidiaries or affiliates, and the products themselves are proprietary to UserGate.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

ClickHouse is a registered trademark of ClickHouse, Inc. https://clickhouse.com/

Zabbix is a registered trademark of Zabbix SIA.

ViPNet is a registered trademark of Infotecs.

The MITRE Corporation Terms of Use

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.