kaspersky

Kaspersky Machine Learning for Anomaly Detection

Contents

About Kaspersky Machine Learning for Anomaly Detection

The early anomaly detection system known as Kaspersky Machine Learning for Anomaly Detection (hereinafter also referred to as Kaspersky MLAD or "the application") is specialized software designed to prevent failures, accidents or degradation of industrial installations, technological processes, and complex cyberphysical systems. By analyzing telemetry data using machine learning techniques (artificial intelligence), Kaspersky MLAD detects signs of an abnormal situation before it is detected by traditional monitoring systems.

Kaspersky MLAD detects anomalies in industrial processes regardless of their causes. Anomalies may be caused by the following:

- Physical factors, such as damage to equipment or malfunctioning sensors.
- Human factors (such as intentional or inadvertent inappropriate actions of the operator, hardware configuration, change of operating modes or equipment, or switch to manual control).
- Cyberattacks.

Main capabilities of Kaspersky MLAD:

- Detects abnormal behavior of the monitored asset in real time.
- Identifies signals that display the largest deviations from normal behavior.
- Allows you to analyze incidents taking into account information about similar incidents.
- Allows expert classification and annotation of incidents.
- Allows you to alert users about detected incidents through the web interface, by email, by sending messages to Kaspersky Industrial CyberSecurity for Networks, and using industrial data transfer protocols.
- Allows you to use models based on both machine learning and arbitrary rules for anomaly detection.
- Displays observed and predicted tag values and prediction errors as the graphs both in the online monitoring mode and in the retrospective analysis of telemetry history mode.
- Lets you manage the log of detected incidents.
- Allows you to perform retraining and additional training of the ML model being used.
- Allows you to create ML models and add elements to it based on neural networks and diagnostic rules.
- Allows to create templates based on the added ML models and add ML models to Kaspersky MLAD based on the created templates.
- Allows you to define the way to organize the data of the monitored asset in the form of an asset tree.
- Allows you to receive telemetry data over HTTP, OPC UA, MQTT, AMQP, CEF, and WebSocket protocols, and via a specialized protocol over HTTPS from Kaspersky Industrial CyberSecurity for Networks.
- Displays historical and real-time data as graphs according to the specified sets of tags.
- Detects and handles terminations and interruptions of the incoming data stream, and restores missed observations.

- Based on data on events received from external systems, recognizes principles as repeated events or patterns, and identifies new events and patterns in the event stream.
- Displays the detected events as a graph and a table, and shows detected patterns as a layered hierarchy of nested items.
- Sends alerts about the detection of certain events, patterns, or values of the event parameters received by the Event Processor in the data stream from the monitored asset.

Distribution kit

Kaspersky MLAD is delivered as an archive file named Kaspersky_MLAD_4.0.2.-<build number>_ru-RU_en-US.tar.xz, which contains the following files:

- Installation script and all files required for system installation.
- Files containing the text of the End User License Agreement in English and in Russian.
- Files containing information about the application (Release Notes) in English and in Russian.
- File containing information about third-party code (legal_notices.txt) in English.

After you unpack the archive, the "legal" directory will contain a text file named license_en.txt in which you can view the End User License Agreement. The End User License Agreement specifies the terms of use of the application.

Hardware and software requirements

> The hardware requirements for each protected facility must be adjusted considering the model being used, the number of processed tags and events, the average speed of data acquisition (number of observations per second), and the volume of stored data. The more data is processed and the more sophisticated the used ML model is, the more hardware resources are required for installing the server part of Kaspersky MLAD.

Requirements for Kaspersky MLAD server

To ensure proper operation of the application, the Kaspersky MLAD server must meet the following minimum requirements.

List of supported processors:

- Intel® Xeon® E3 v3, v4, v5, v6
- Intel Xeon E5 v3, v4
- Intel Xeon E7 v3, v4
- Intel Xeon Scalable processors
- The 2nd and 3rd generation Intel Xeon Scalable processors

- Intel Xeon E
- Intel Xeon W
- Intel Xeon D
- The 4th generation and later Intel Core™ i5, i7
- Intel Core i9 processor
- Intel Core M

Minimum hardware requirements:

- 8 cores
- 32 GB of RAM
- 200 GB of free space on the hard drive (SSD recommended)
  If Kaspersky MLAD receives a large data stream, increase the amount of free space on the hard drive.

You can install Kaspersky MLAD on a server with another x86 64-bit processor released in 2013 or later. The processor must meet the minimum hardware requirements listed above and support the following extensions required for the TensorFlow™ 2.13 library:

- Advanced Vector Extensions (avx)
- Advanced Vector Extensions 2 (avx2)

Supported operating systems:

- Ubuntu 22.04 LTS or later

The following software must be installed prior to deployment of Kaspersky MLAD:

- docker 20.10.21 or later
- docker compose 2.12.2 or later

> Use the official Docker repository for installation of the software on the Kaspersky MLAD server.

User computer requirements

To work with the web interface of Kaspersky MLAD, the user's computer must meet the following minimum requirements:

- Intel Core™ i5 CPU
- 8 GB of RAM
- 64-bit operating system
- Google Chrome™ browser version 107 or later

- The minimum screen resolution for correct display of the web interface is 1600x900.

Security recommendations

To ensure secure operation of Kaspersky MLAD at an enterprise, it is recommended to restrict and control access to equipment on which the application is running.

Physical security of equipment

When deploying Kaspersky MLAD, it is recommended to take the following measures to ensure secure operations:

- Restrict access to the room housing the server with Kaspersky MLAD installed, and to the equipment of the dedicated network. Access to the room must be granted only to trusted persons, such as personnel who are authorized to install and configure the application.
- Employ technical resources or a security service to monitor physical access to equipment on which the application is running.
- Use security alarm equipment to monitor access to restricted rooms.
- Conduct video surveillance in restricted rooms.

Information security

ML model parameters directly impact the detection of anomalies, therefore they can only be changed by system administrators. The date of last modification to the ML model (activation, or change of the name, threshold MSE value or MSE weights) is available in the **Models** section. The change history is available only in logs, which are saved for only a limited amount of time.

When using the web interface, it is recommended to take the following measures to ensure the data security of the intranet system:

- Provide users with access to the application through the web interface only.
- Install certificates to users' computers for authorization of the Kaspersky MLAD server with their browser. To use a trusted certificate, you need to contact a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.
- Ensure protection of traffic within the intranet system.
- Ensure protection of connections to external networks.
- Use a secure TLS connection for data transfer.
- Change the name and password of the first application user with the system administrator role when installing the application.
- For connections through the web interface, use passwords that meet the following requirements:
  - Must not match previously used account passwords. The specific number of most recently used passwords that must not be reused is defined when configuring the application security settings.

  - Must contain at least 8 characters.
  - Must contain one or more uppercase letters of the English alphabet.
  - Must contain one or more lowercase letters of the English alphabet.
  - Must contain one or more numerals.
  - Must contain one or more of the following special characters: _ ! @ # $ % ^ & *.

- Ensure that passwords are confidential and unique. If the password has been possibly compromised, change the password.
- Set a time limit for a user web session.
- After you are finished working in the browser, manually terminate the application connection session by using the **Sign out** option in the web interface.
- Periodically install updates for the operating system on the server where Kaspersky MLAD is deployed.
- Use access permission control to restrict user access to application functions.

Data security

While working with Kaspersky MLAD, it is recommended to take the following measures to ensure data security:

- Configure the operating system and provide the necessary access to files of the server where Kaspersky MLAD is installed in accordance with the *Recommendations on secure configuration of Linux operating systems* issued by the Federal Service for Technical and Export Control (FSTEC) of Russia.
- Perform periodic data backups of the server that has Kaspersky MLAD installed in accordance with the internal company procedure.
- Periodically test the performance of the interface and services of the application. Special attention should be directed to the notification service and logging system.
- Check communication channels to make sure they are secure and working properly.
- Periodically test the performance of the server:
  - SMART disk check
  - Availability of sufficient free space and memory
  - RAM utilization
- Use the monitoring system to make sure that there are no problems with the server protocols.
- Store sensitive data in a secure storage location.

Fixing vulnerabilities and installing critical updates

Kaspersky may release application updates aimed at eliminating vulnerabilities and security flaws (critical updates). Urgent update packages are supplied and installed in accordance with the current *Technical Support Agreement*. Notifications regarding the release of critical updates are sent to the email addresses specified in the current *Technical Support Agreement*.

It is recommended that the personnel responsible for application operation also periodically (at least once every three months) verify the absence of detected vulnerabilities in the application by referring to the Kaspersky website ↗.

You can report security flaws or program vulnerabilities with a PGP™-encrypted message to vulnerability@kaspersky.com ↗. Please provide the following information in your email:

- Your contact details.
- The product name, version, and type of operating system installed on the asset where the vulnerability was found.
- A detailed description of the vulnerability.
- Any plans to share information about the vulnerability with a third party.

> Do not publish any information about the vulnerability until fixed by Kaspersky.

Managing access to application functions

This section describes user access restrictions for application functions.

In Kaspersky MLAD, you can use roles to restrict users' access to application functions depending on the tasks performed by users.

A *role* is a set of rights to access application functions that you can assign to a user.

Depending on the assigned role, users may have access to the following functions of Kaspersky MLAD:

Accessible functions of the application

Functional scope	System administrator	User role
Managing user accounts: • Creating and editing a user account • Revoking authentication tokens for a user account • Viewing rights for a user account	✓	–
Managing roles: • Creating and changing a role • Deleting role • Viewing access rights for a role	✓	–

Viewing the rights of users	✓	–
Managing incident notifications: • Creating, editing, and deleting incident notifications • Enabling and disabling sending notifications about incidents	✓	–
Configuring Kaspersky MLAD	✓	–
Managing assets: • Creating and modifying an asset • Creating a tag and adding a tag to an asset • Editing a tag • Moving assets and tags • Deleting an asset or tag • Checking the current structure of tags • Importing and exporting asset configurations	✓	–
Managing ML models: • Uploading an ML model • Activating an imported ML model • Creating an ML model • Changing an ML model • Adding and modifying a neural network element of an ML model • Adding and modifying an ML model element based on a diagnostic rule • Removing an ML model element • Cloning an ML model • Creating and modifying a template based on an ML model • Creating an ML model based on a template • Removing an ML model template • Training elements of an ML model and viewing the results of training ML model elements • Preparing an ML model for publication • Publishing an ML model	✓	✓ (by appointment)

• Removing an ML model		
Managing Kaspersky MLAD services: • Viewing the statuses of services • Starting, stopping, and restarting services	✓	✓ (by appointment)
View Kaspersky MLAD logs.	✓	✓ (by appointment)

All application users have the following default rights:

- Viewing summary data in the **Dashboard** section
- View primary and operational data by tags in the **History** and **Monitoring** sections
- Viewing the values of the process parameters received from the monitored asset's sensors at a certain point in time in the **Time slice** section.
- Working with events and patterns:
  - Configuring attention settings and display of event parameters
  - Creating and deleting monitors
  - Viewing the event and pattern history
- Working with incidents and groups of incidents:
  - Viewing incidents and incident groups
  - Adding a status, cause, expert opinion or note to an incident or incident group
  - Exporting incidents to a file
- The following actions in the **Models** section:
  - Creating, modifying, and deleting markups
  - Starting and stopping ML model inference
  - Viewing the data flow graph of an ML model
- Manage presets:
  - View presets
  - Create, modify, and delete models
  - Load a preset configuration from a file
  - Save a preset configuration to a file
- Change your own password

You can also create a role with a **Rights to all actions** permission. Users with this role have access to system administrator functions.

You can view the available user roles and their access rights to application functions in the **Roles** section of the administrator menu.

You can view application functionality access rights for specific users in the **Users** section of the administrator menu.

What's new

Kaspersky Machine Learning for Anomaly Detection 4.0 has the following new capabilities and improvements:

- Model builder: Functionality has been added that allows you to create, modify, and delete your own ML models and elements of ML models based on a neural network and/or diagnostic rules.
- Markups: Functionality has been added that allows you to create, modify, and delete markups for training and inferencing ML models.
- Training ML models: The capability to manage the settings for training ML model elements has been added to the application web interface. You can also start or interrupt the training of ML model elements, view the number of the current element training epoch and view the results of the last training process in the program web interface.
- Monitored asset hierarchical structure: Functionality has been added that allows you to define the way in which the assets of the monitored asset are organized in the form of a tree of primary and functional elements in Kaspersky MLAD. The primary elements of the hierarchical structure are represented by assets and tags, which can be managed in the **Assets** section. The format of the configuration file for downloading tags has been changed to XLSX. When the configuration file is downloaded, the assets of the hierarchical structure are also downloaded. The functional elements of the hierarchical structure are represented by ML models, ML model templates and markups. The monitored asset hierarchical structure is displayed in the **Assets** and **Models** sections, as well as in the **Presets** section when creating or modifying presets.
- Roles: Functionality has been added that allows you to manage roles and select access rights to application functions for them. Role management is available in the **Roles** section.
- Security policy: Functionality has been added that allows you to manage the security settings of Kaspersky MLAD in accordance with the security policy at the enterprise.
- Information security event logging: Functionality has been added that allows you to manage the storage settings of information security event logs, as well as view information security event logs in the Grafana logging system.
- Application update script: Functionality has been added that allows you to back up Kaspersky MLAD and restore the application from the backup copy using the application update script. Changed the command for starting the script to update the application whenever new versions have been released.
- CEF Connector: Functionality has been added that allows you to send information security event logs to an external system.
- OPC UA Connector: Added new settings for configuring the OPC UA Connector.
- Mail Notifier Service: Added new settings for configuring the Mail Notifier service.
- Trainer service: Trainer service has been optimized.
- Kaspersky MLAD web interface was updated.
- Added new settings for configuring the display of graphs under **Monitoring** and **History**.

Basic concepts of Kaspersky MLAD

This section contains expanded definitions of the basic concepts applied in Kaspersky MLAD.

Monitored asset hierarchical structure

The *monitored asset hierarchical structure* (also simply referred to as the *hierarchical structure*) is a method of organizing monitored asset data in the form of a tree, whose leaf nodes correspond to source tags and/or tags processed by the Stream Processor service.

Monitored asset tags are organized as a hierarchy of assets representing units, plants, shops, and factories. The number of assets depends on the structure of a specific monitored asset. Each asset has only one parent element. This element can be another asset (parent asset) or a head element of the hierarchical structure that corresponds to the monitored asset as a whole.

Tags and assets are the primary elements of a hierarchical structure. You can import or export an asset tree as an XLSX file, and create and manage them in the **Assets** section.

In addition to primary elements, the following functional elements can be added to the hierarchical structure in the process of or as a result of the operations of Kaspersky MLAD:

- Markups
- ML models
- Templates for ML models

Tags

Tags are the main objects of observation in Kaspersky MLAD. A *tag* is a process parameter transmitted within the industrial network (for example, a controlled temperature). Measurements of physical parameters, as well as setpoints, commands, or states of control systems can be transmitted as tags. The values of tags are transmitted and received by the assets over specific protocols. The values of tags are displayed on graphs in the **History** and **Monitoring** sections and are also used to detect incidents.

Kaspersky MLAD provides the following types of tags:

- **Source tags**

  The values of these tags are received by Kaspersky MLAD directly from the monitored asset if the Stream Processor service is disabled.

  Source tags are displayed in the monitored asset hierarchical structure.

- **Tags processed by the Stream Processor service**

Tag values received as a result of the processing of the input tag stream by the Stream Processor service.

The Stream Processor service can convert an input tag stream to a UTG. For each node in the uniform sequence, the Stream Processor service calculates the tag values for the output stream. Depending on how many input observations have been accumulated for each node and how long ago the observations were last received, the Stream Processor service can calculate output tag values by aggregation (calculating a tag value based on multiple tag observations accumulated for the corresponding node of the uniform sequence) or imputation (restoring the tag value for an empty node of the uniform sequence based on the values of this tag received earlier).

The Stream Processor service can also calculate derivative tags based on incoming telemetry data. For example, the Stream Processor service can calculate a moving average or an average for a group of tags.

Tags processed by the Stream Processor service are displayed in the monitored asset hierarchical structure.

Kaspersky MLAD supports several methods for obtaining telemetry data (tags). Depending on the monitored asset attributes and the tag transmission capabilities, you can select one of the following methods for receiving tags:

- Use the connectors of Kaspersky Industrial CyberSecurity for Networks that analyze mirrored traffic and send tags to Kaspersky MLAD in online mode. Kaspersky MLAD sends back information about detected incidents.
- Use the **OPC UA Connector** if the monitored asset provides the capability to transmit tags from ICS over the OPC UA protocol in the online mode.
- Use the **MQTT Connector** if the monitored asset provides the capability to transmit tags over the MQTT protocol and receive alerts about incident registration in the online mode.
- Use the **AMQP Connector** if the monitored asset has the capability to transmit tags over the AMQP protocol and receive alerts about incident registration in online mode.
- Use the **WebSocket Connector** if the monitored asset provides the capability to transmit tags over the WebSocket protocol and receive alerts about incident registration in the online mode.
- Use the **CEF Connector** if the monitored asset provides the capability to transmit tags using the CEF Connector technology and receive alerts about incident registration in the online mode.
- If the first four methods of tag transmission are not available, you can write a tag export script for using the **HTTP Connector** to configure a scheduled export of tags as CSV files over HTTP (for example, once per hour or once per minute).

ML models

An *ML model* is an algorithm based on machine learning methods tasked with analyzing the telemetry of the monitored asset and detecting anomalies.

An ML model is created for a specific monitored asset while taking into account the specifications of the asset and the characteristics of telemetry data. The general structure of the algorithm (architecture) is formed during creation of the ML model. Then the ML model is trained based on historical telemetry data and is thereby adjusted to the behavior of a specific object.

An ML model consists of one or several elements, each of which is an independent ML model. The overall result of the Anomaly Detector service is formed by combining the results of the ML model elements inference. Normally, the more complex the industrial processes of the monitored asset are, the more elements the ML model will contain.

Inference is the process of running telemetry data in an ML model to identify anomalous behavior. In Kaspersky MLAD, ML model inference can be performed on historical data (*historical inference*) and on telemetry data received in real time (*streaming inference*). If historical inference is started for multiple ML models, Kaspersky MLAD runs the inference of these ML models in the order of their startup queue. The duration of historical inference is determined by the time interval of the data analyzed by the ML model. If streaming inference is started for multiple ML models, Kaspersky MLAD runs the inference of these ML models simultaneously. Historical inference and streaming inference run in parallel and independently of each other.

During the inference process, the ML model registers incidents that can be viewed in the **Incidents** section.

ML models can be created by Kaspersky specialists or by a certified integrator as part of the *Kaspersky MLAD Model-building and Deployment Service*. To use such ML models, you must download them to Kaspersky MLAD. You can also create ML models independently and add the necessary elements to them using the model builder.

An ML model can include the following elements operating in parallel:

- Element based on a neural network
- Element based on a diagnostic rule

In Kaspersky MLAD, a ML model can be assigned one of the following statuses:

- *Not activated*: the ML model is imported but is not activated.
- *Draft*: the ML model is activated, or the ML model is created manually and contains untrained neural network elements.
- *Trained*: all the elements in the ML model are trained. Inference can be run on a trained ML model.
- *Ready for publication*: the ML model is prepared for publication and cannot be modified.
- *Published*: the ML model has been published. Inference can be run on a published ML model.

Element of an ML model based on a neural network

The most common type of ML model is a neural network, which predicts the behavior of an object based on data from its behavior in the recent past. This ML model is based on the Forecaster detector.

If the difference between the model prediction and the actual observed values exceeds a certain threshold, the Forecaster detector detects an anomaly in the monitored asset behavior and registers an incident. The cumulative indicator of the difference between the predicted values and the actual values (cumulative prediction error) is referred to as the *MSE* (*mean squared error*) in the user interface.

The MSE values graph and the MSE threshold which, when exceeded, causes the Forecaster to detect an incident, are displayed in the **Monitoring** and **History** sections under the tag graphs. If an ML model contains multiple elements, you can select a model element to view the MSE values calculated by that element.

Kaspersky MLAD model builder supports the following neural network architectures for elements of an ML model:

- *Dense*. Element of an ML model with a fully connected architecture. When creating an ML model element, you must specify the multipliers for calculating the number of neurons on inner layers and the activation functions on them.
- *TCN*. Element of an ML model with a hierarchical time-based convolutional architecture. When creating an ML model element, you must specify the activation function, filter size, extensions on layers, and the number of encoders.
- *CNN*. Element of an ML model with a convolutional architecture. When creating an ML model element, you must specify the number of convolutional layers, the size and number of filters on layers, and the size of the maximum sampling window (MaxPooling).
- *RNN*. Element of an ML model with a recurrent architecture. When creating an ML model element, you must specify the number of GRU neurons on layers and the number of time-distributed neurons on the layers of the decoder.
- *Transformer*. Element of an ML model with a transformer architecture. When creating an element of the ML model, the number of attention heads and the number of transformer encoders are specified.

Element of an ML model based on a diagnostic rule

Diagnostic rules describe previously known behavioral traits of the monitored asset that are considered anomalies. Diagnostic rules must be formalized and calculated based on available telemetry data for the object. Diagnostic rules are based on the Rule Detector.

Diagnostic rules are formulated by subject-area experts and are implemented by Kaspersky experts or a certified integrator as a JSON file in a serialized rule structure format. You can also formulate diagnostic rules on your own using the model builder.

Examples of diagnostic rules:

- The value of tag A does not change over the course of one minute.
- Over the past 12 hours, tag B has trended upward, tag C has trended downward, and tag D has not shown any clear dynamics.
- The value of tag X fell below 2800 after it previously rose higher than 2900.

ML model templates

ML model templates are created on the basis of ML models previously added to Kaspersky MLAD or created using the model builder functionality. ML model templates preserve the algorithm structure, set of elements, and the state of the ML model used to create the template. The training state of the created ML model will match the training state of the source ML model when the template was created.

Using templates, you can add ML models of the same type to Kaspersky MLAD. These models will analyze data received from equipment of the same type with a similar set of tags. When creating an ML model from a template, you can configure the use of other tags in the ML model by specifying tag IDs that differ from the ones in the source ML model.

Markups

A *Markup* is a set of time intervals specified for Tags according to certain rules. Markups are used to generate learning indicators and inference of the ML model. Markups that form part of learning indicators define the data time intervals from which the ML model takes data for training. Markups that form part of inference indicators define the time intervals during which the ML model performs the inference.

Markup is a functional element of the hierarchical structure. Markups can be imported into Kaspersky MLAD together with an ML model, or they can be manually created.

Incidents

An *incident* is a deviation from the expected (normal) behavior of a monitored asset identified by the anomaly detector.

Kaspersky MLAD supports multiple types of anomaly detectors: Forecaster, Rule Detector, and Limit Detector. The Forecaster Detector serves as the foundation for neural network elements of an ML model, while diagnostic rules are based on the Rule Detector. Each detector analyzes incoming telemetry data received from the monitored asset to identify deviations from normal behavior of the asset.

In addition to detecting deviations from normal object behavior, Kaspersky MLAD monitors the quality of incoming data. If the input data stream is terminated or interrupted for a specific tag, or observations that arrived at the application too soon or too late are detected in the input stream, the Stream Processor service registers incidents.

When a deviation is detected, the corresponding detector records the date, time and relevant deviation parameters, and saves this data as an entry in the **Incidents** section. If incident notifications for users or external systems are configured in Kaspersky MLAD, information about an incident is sent to the intended recipients via the corresponding services of Kaspersky MLAD.

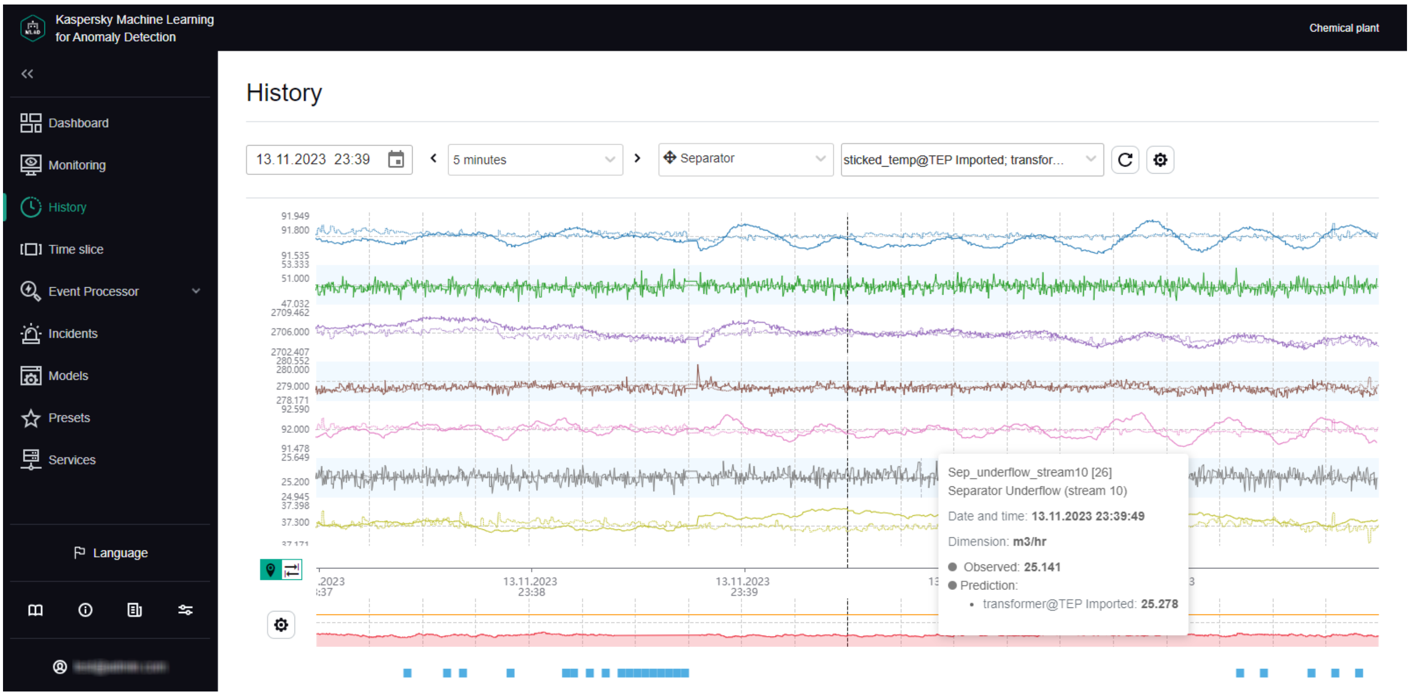
Incidents detected by a neural network element of an ML model

An ML model neural network element based on the *Forecaster* detector is trained on a specific subset of tags and can predict the current behavior of tags. In this case, an incident is any substantial discrepancy between the observed (actual) values of tags and the predicted values of tags resulting from operations of the ML model element. In the model element settings, you can view which tags are analyzed by the neural network (**Input tags** parameter) and which tags' behavior is predicted (**Output tags** parameter).

An ML model built based on the Forecaster detector consists of one or several ML model elements that operate in parallel. In the **History** and **Monitoring** sections, you can select a specific branch of the ML model to display the incidents registered as a result of a specific model element operation on the MSE graphs. Registered incidents are displayed as color-coded dot indicators in the lower part of the MSE graph.

The MSE graph also displays the predicted tag values and MSEs for the selected element of the ML model. *MSE (mean square error)* is an indicator of the difference between predicted values from actual values, calculated cumulatively for all tags included in the selected element of the ML model. The higher the MSE value, the more the behavior of tags will differ from the expected (normal) behavior. *The MSE threshold* is the critical MSE value that, when exceeded, causes the Forecaster detector to register an incident. The MSE threshold on an MSE graph is shown as an orange line.

The MSE graph is displayed in the lower part of the **History** section (see the figure below).



History

13.11.2023 23:39 · 5 minutes · Separator · sticked_temp@TEP Imported; transfor...

Sep_underflow_stream10 [26]
Separator Underflow (stream 10)
Date and time: **13.11.2023 23:39:49**
Dimension: **m3/hr**
● Observed: **25.141**
● Prediction:
- transformer@TEP Imported: **25.278**

MSE graph in the **History** section

For each incident, the application automatically identifies the tags whose behavior had a stronger influence on incident registration. These tags are used to form the Tags for event #N preset, which is available for selection in the **History** section. Tags that are included in the Tags for event #N preset are sorted in descending order of their deviation from expected behavior. The first, most anomalous tag is also displayed in the incidents table in the **Incidents** section. The incidents table also indicates the MSE threshold and the actual MSE value at the moment when the incident was registered.

Information obtained when viewing the Tags for event #N preset is not actually diagnostic information for the purposes of identifying the causes of an incident, but you can still use this information when analyzing the values of tags with the largest deviations in behavior. The tag whose behavior was the first to deviate from the norm and caused subsequent deviations in other tags is referred to as the causal tag. In some cases, the causal tag may not be at the top of the list in the Tags for event #N preset and may even be entirely absent from this preset. This could happen due to the following reasons:

- Minor amplitude changes in the behavior of the causal tag had a multiplier effect and caused significant deviations in other tags that were included in the Tags for event #N preset.
- The causal tag is not analyzed by the ML model, and Kaspersky MLAD registers derivative changes in the behavior of tags caused by the deviation of the causal tag.
- Changes in the behavior of the causal tag had a delayed effect, and by the time an anomaly occurred in the operation of the monitored asset, the behavior of the causal tag returned to normal.

Incidents detected by an ML model element based on a diagnostic rule

An ML model element based on a diagnostic rule consists of one or more diagnostic rules. This element is based on the Rule Detector. Each diagnostic rule results in the following values being obtained that are calculated at each point in time:

- Value `0`. The diagnostic rule was not triggered or applied at this moment.
- Value `1`. The diagnostic rule was triggered at this moment.

- Intermediate values from `0` to `1` are possible in individual cases. The diagnostic rule was partially triggered at this moment.

Whenever the received value reaches the threshold defined for a diagnostic rule (normally equal to 1), the Rule Detector registers an incident. For each incident registered by the Rule Detector, the application automatically creates the "Tags for event #N" preset, which is available in the **History** section. This preset contains the value obtained as a result of the work of the diagnostic rule, as well as the tags included in this rule.

To display graphs of values obtained as a result of the work of diagnostic rules, you can enable the display of predicted values of tags in the **History** section.

Incidents detected by the Limit Detector

If the *Limit Detector* is enabled, Kaspersky MLAD automatically monitors all tags having blocking thresholds specified for the tag when using any ML model. Blocking thresholds can be defined in a tag configuration imported into Kaspersky MLAD at the start of operations. You can change the tag blocking thresholds when editing a tag.

To visually control the position of a tag graph relative to its blocking thresholds, enable the **Always display blocking threshold** option. If this option is disabled, the upper or lower threshold line is displayed only if the tag values have reached the corresponding threshold during the time interval displayed on the screen. The Limit Detector identifies and registers events regardless of whether or not the **Always display blocking threshold** option is enabled.

When the tag value reaches its upper or lower technical limit, the Limit Detector registers an incident. This tag is displayed in the incidents table in the **Incidents** section. The incidents table also shows the blocking thresholds of the tag and the actual value of a tag that violated one of these limits. For each incident registered by the Limit Detector, the application automatically creates the "Tags for event #N" preset, available in the **History** section. This preset includes the only causal tag of the incident.

Incidents detected by the Stream Processor service

The *Stream Processor* service gathers real-time telemetry data received from the monitored asset at arbitrary points in time and converts this data to a uniform temporal grid (UTG). When analyzing incoming data, the Stream Processor service can detect losses of telemetry data and observations that were received by Kaspersky MLAD too early or too late. The Stream Processor service registers an incident in such cases.

Incidents detected by the Stream Processor service are displayed in the incidents table of the **Incidents** section. Each incident registered by the Stream Processor service is automatically assigned one of the following incident types:

- **Clock malfunction** – observations received by Kaspersky MLAD too early are detected.

- **Late receipt of observation** – observations received by Kaspersky MLAD too late are detected.

- **No data** – input data stream for a specific tag was terminated or interrupted.

The Stream Processor service transfers the UTG-converted data to the ML model of the Anomaly Detector service.

Anomalies

An *anomaly* is any deviation in a monitored asset's behavior that is abnormal, not provided for by the current work procedure, and not normally caused by the industrial process.

Kaspersky MLAD registers only incidents. A specific incident can be identified as an anomaly only by an ICS specialist after conducting an analysis of incidents registered by the application. An incident analysis may result in one of the following conclusions:

- The incident is an anomaly that requires certain actions from a responding operator of the monitored asset.
- **The incident is not actually an anomaly, but instead was a false positive by the triggered detector**.

  > If the detector is persistently triggered by recurring false positives, you need to identify the reason for the deteriorating quality of the detector used in the ML model, perform additional configuration, or conduct additional training of the ML model. Additional configuration of a detector or additional training of an ML model is performed by Kaspersky experts as part of the *Kaspersky MLAD Model-building and Deployment Service*.

- **The detector utilized in the ML model was correctly triggered but the incident is not an anomaly**.

  > The incident was a result of temporarily switching the monitored asset to a non-standard operating mode (preventative maintenance or testing) or was caused by short-term impacts from non-standard external factors (unusual weather conditions or startup of a neighboring unit). In this case, there is no need for any responsive actions from an operator of the monitored asset.

Incidents are analyzed and assessed by a subject-matter expert. In some cases, like when registering incidents detected by diagnostic rules or incidents that occur repeatedly, similar incidents can be automatically grouped and assessed.

The detector utilized in the ML model may fail to detect an actual anomaly. In this case, the anomaly will not be correlated to any registered incidents and will not be reflected in the Kaspersky MLAD history. If according to the expert or operator observations or external sources a detector is repeatedly not triggered, you need to identify the reason for the deteriorating quality of the detector, perform additional configuration, or conduct additional training of the ML model. Additional training of the ML model can be performed only by Kaspersky experts or certified integrators.

New events, patterns, and values of the event parameters detected by the Event Processor service in the stream of incoming events can also indicate an anomaly in the operation of a monitored asset. When new events, patterns or values of event parameters are detected, the Event Processor service does not register incidents. To view new detections in the **Event Processor** section, you can view the history of registered patterns, filtering them by the **New** type. You can also create a monitor for tracking new events, patterns, or values of event parameters. The Event Processor service activates the monitor when it detects events, patterns, or event parameter values that match the specified search criteria. When the specified threshold for the number of monitor activations in a sliding window is reached, the Event Processor service sends an alert about the monitor activation to the external system using the CEF Connector.

Event Processor

The Kaspersky MLAD Event Processor is designed to detect regularities in the form of recurring events and patterns in the stream of events received from monitored assets and from the Anomaly Detector service, as well as to detect new events and patterns. New events and patterns may indicate an anomaly in the monitored asset operation.

Events

Data received from monitored assets and from the Anomaly Detector service are processed as events by the Event Processor service. An *event* is a set of values describing a change in the monitored asset state according to a predefined list of parameters and the time when this change occurred. The set of event parameters depends on the monitored asset and is defined in the configuration file for the Event Processor service.

The Event Processor is designed to work only with categorical values of the event parameters. Event parameter values are converted to string type. Kaspersky MLAD uses the Anomaly Detector service to work with numeric values of telemetry data when processing the event stream. The system administrator can enable the processing of data received from the Anomaly Detector service when configuring the Event Processor service settings.

An event is a phenomenon distinct from other events. There may also be intervals of time during which no events have occurred. Event registration may be affected by such factors as the actions of personnel, changes in the asset operating mode at the facility, or the execution of ICS commands by a specialist.

Examples of situations that may lead to event registration in Kaspersky MLAD

Event examples are provided for various monitored assets.

- *Employee login.*
  - Event time: 11/10/21 09:03
  - Event parameters:
    - Source: ACS
    - Employee: Smith
    - Station: engine room door, exterior side
    - Result: Passage.
- *Unit startup.*
  - Event time: 11/10/21 09:09
  - Event parameters:
    - Source: Operator workstation
    - User: Smith
    - Equipment: Unit 1
    - Command: Ignition switched on
    - Current: 44 A
    - Duration: 10 seconds.
- *Mode activation.*
  - Event time: 11/10/21 09:24
  - Event parameters:
    - Source: ICS
    - Equipment: Unit 1
    - Nominal mode: True.

An event is registered once by the Event Processor service. When an event stream is received, the Event Processor recognizes previously detected events. If events are found that do not match those previously detected, the Event Processor registers new events.

You can view the received events as a graph or a table. To view events, you need to upload them to **Event Processor** → **Event history**. Event parameters specified in the configuration file for the Event Processor service may not appear in all events received from the monitored asset. Thus, some parameters may be missing when you view the received events.

Patterns

The Event Processor detects regularities in the stream of events arriving from the monitored asset. These regularities are detected as a hierarchy of stable (persistently recurring) patterns, which can be either *simple patterns* (sequences of events) or *composite patterns* (sequences of patterns). The patterns that form a composite pattern are called subpatterns.

A sequence of events or patterns is considered recurrent if its constituent elements follow the same order, and the time intervals between similar elements in different sequences differ from each other by no more than a specific maximum range. The allowable range of intervals between the pattern elements is calculated considering the value of the **Coefficient defining the permitted dispersion of the pattern duration** parameter. Patterns are the result of the specific facility's adopted practices, prescribed procedures, or technical specifics of the industrial process.

The Event Processor presents the detected regularities as a layered hierarchy of nested elements (pattern structure) down to the event level. Events are the first layer elements, simple patterns are the second layer elements, and composite patterns are the third and higher layer elements. Event parameter values are elements of the null layer.

A pattern is registered once by the Event Processor service. When an event stream is received, the Event Processor recognizes previously detected patterns. If patterns are found that do not match previously detected regularities, the Event Processor registers new patterns.

New patterns also include the sequences of events or patterns with a deviation in the order or composition of subpatterns (for example, turning on an industrial unit before the operator has arrived at the workstation) or with significant changes in the intervals between events or subpatterns even though their sequence is preserved (for example, turning on an industrial unit immediately after or a lot later than the operator arrived at the workstation). Thus, the Event Processor registers patterns with a new structure.

New patterns may indicate an anomaly in the monitored asset operation. You can view the structure of the new pattern and examine its deviations from the structure of previously detected patterns.

If a newly identified sequence of events or patterns begins to repeat in a persistent manner, this sequence is converted to a stable pattern.

Attention directions

The event stream from the monitored asset usually contains many unrelated events. The Event Processor service supports an attention direction mechanism to detect patterns based on a specific subset of events from the entire stream.

Attention is a special configuration of the Event Processor intended to track events and patterns for specific subsets of event history (attention directions). An attention direction is defined by the event parameter value that is common for all events of this direction. The Event Processor detects events and patterns only for the attention directions defined in the attention settings.

You can configure attention directions in the **Event Processor** section.

Event Processor operating modes

Kaspersky MLAD has the following operating modes of the Event Processor service:

- **Online mode**. In the online mode, the Event Processor processes the incoming stream as episodes. An *episode* is a sequence of events from the entire stream that is limited by a specific time period and/or the number of events. An episode is formed when one of the following conditions is fulfilled:

  - The episode accumulation time reached the limit defined by the **Interval for receiving batch events (sec.)** parameter of the Event Processor service.

  - The number of accumulated events reached the limit defined by the **Batch size in online mode (number of events)** parameter of the Event Processor service.

  Based on an episode received in the event stream, the Event Processor service detects new and/or repeated (stable) events and patterns for each of the specified attention directions. You can configure attention directions in the **Event Processor** section.

  When an event with the timestamp belonging to a previously processed episode is received, the Event Processor service does not revise the structure of patterns detected during the processing of that episode. The Event Processor service takes into account the events received by Kaspersky MLAD with a delay when detecting patterns during the event history reprocessing in the sleep mode.

- **Sleep mode**. To improve the quality and structure of the identified patterns, the Event Processor can switch to sleep mode according to the specified schedule. Processing of the event stream in the online mode is paused, and Kaspersky MLAD accumulates incoming events in the internal limited buffer on the server for subsequent processing after the application switches from the sleep mode back to online mode.

  In sleep mode, the Event Processor re-analyzes sequences of events that were previously processed in online mode. To detect more complex pattern structures in the sleep mode, the Event Processor processes sequences of events during longer time intervals than the episode accumulation time in the online mode.

  In the Event Processor service settings, you can configure a schedule for the sleep mode (for example, at the time when the event stream is least intense) and define a time interval for the events analyzed in the online mode to be forwarded for reprocessing in the sleep mode.

Monitors

A *monitor* is the source of notifications about patterns, events, or values of event parameters detected by the Event Processor according to the defined monitoring criteria. The monitoring criteria define a sliding time interval, the number of sequential detections, filters for event parameter values, and the condition for detecting new events, patterns, or event parameter values.

You can create monitors for alerts about the following detections in the event stream:

- **Values of event parameters**. You can create a monitor for alerts about the identification of new or previously encountered values of a specific event parameter. For example, to track new users on a monitored asset, create a monitor with the **Parameter values** subscription type and configure it to detect new values for the **User** parameter.

- **Events**. You can create a monitor for alerts about the identification of new or previously encountered events. You can also focus the attention of the Event Processor on a specific parameter of events. For example, to track new actions of a specific user at the monitored asset, you need to create a monitor with the **Events** subscription type and specify the name of the user whose actions you want to track in the **User** event parameter.

- **Patterns**. You can create a monitor for alerts about the identification of new or previously encountered patterns based on a specific attention direction. For example, to track regularities in the actions of a specific user at the monitored asset, create a monitor with the **Patterns** subscription type, focus the attention of the Event Processor on the **User** parameter, and set this parameter to the name of the user whose actions you want to track.

You can set fuzzy filters in the monitoring criteria. For example, you can create a monitor to track situations when a user (monitoring all values of the **User** parameter) accessed the accounting server (the value of the **Server** parameter) more than ten times (the value of the **Threshold** field) in the last five minutes (the value of the sliding time interval).

When events, patterns, or event parameter values matching the monitoring criteria are detected in the stream of incoming data, the Event Processor activates the monitor. Kaspersky MLAD displays information about the number of monitor activations when viewing a monitor, and sends to the external system alerts about the activation of monitors when the specified threshold is reached for a sliding window using the CEF Connector.

The custom monitors are displayed in the **Event Processor** section on the **Monitoring** tab.

Kaspersky MLAD architecture

Kaspersky MLAD is installed on a server that meets the hardware and software requirements. The Kaspersky MLAD Server centrally stores information about application services and connectors and provides a single web user interface for managing them.

> Access to individual services or application connectors is not provided.

When installing Kaspersky MLAD, all application connectors and services are hosted on the same server and interact with each other through an internal virtual network that is isolated from external systems.

Kaspersky MLAD includes specially prepared ML models, and the following services and connectors:

ML model

An *ML model* is a model created for a specific facility based on machine learning algorithms and/or diagnostic rules using telemetry data from this facility. The ML model detects incidents.

An ML model can be provided as part of the *Kaspersky MLAD Model-building and Deployment Service* or created using the model builder.

Kaspersky MLAD services

Kaspersky MLAD services comprise a set of core application services supplied to each monitored asset. Kaspersky MLAD includes the following services:

- *Anomaly Detector*. Uses an ML model to process data and detect anomalies.
- *Event Processor*. Uses machine learning methods based on a semantic neural network to identify patterns and anomalous sequences of events.
- *Stream Processor*. Brings telemetry data received from the monitored asset at arbitrary real-time moments to a uniform temporal grid.
- *Trainer*. Performs repeated or additional training of an existing ML model based on the new telemetry data obtained by Kaspersky MLAD for a specific monitored asset.
- *Similar Anomaly*. Identifies and groups together similar incidents.
- *Message Broker*. Exchanges data between Kaspersky MLAD services.
- *Time Series Database*. Stores time series of observed tag values, tag values predicted by the ML model, and prediction errors.
- *Keeper*. Performs routing of the telemetry data that should be saved in the database.
- *Database*. Stores all configuration settings of Kaspersky MLAD.
- *API Server*. Supports operation of the internal interfaces of Kaspersky MLAD.
- *Web Server*. Supports operation of the Kaspersky MLAD web interface.

- *Logger*. Stores Kaspersky MLAD operation logs.
- *Mail Notifier*. Sends emails with incident registration notifications.

Connectors

Connectors are services that facilitate the exchange of data with external systems. For each protection object, you must select one of the following connectors:

- *KICS Connector*. Supports interaction with Kaspersky Industrial CyberSecurity for Networks version 4.0 and later.
- *OPC UA Connector*. Receives tags from industrial process control systems (ICS) according to the protocol described in the OPC Unified Architecture specification.
- *CEF Connector*. Receives events from external sources (Industrial Internet of Things, network devices and applications) and returns messages in CEF (Common Event Format) registered by event analysis monitors.
- *MQTT Connector*. Receives tags from ICS and sends messages about incidents via the MQTT (Message Queuing Telemetry Transport) protocol.
- *AMQP Connector*. Receives tags from ICS and sends messages about incidents via AMQP (Advanced Message Queuing Protocol).
- *WebSocket Connector*. Receives tags from ICS and sends messages about incidents via the WebSocket protocol.
- *HTTP Connector*. Receives telemetry data from ICS in CSV files via HTTP POST requests.

The figure below shows a diagram of interaction between Kaspersky MLAD services.

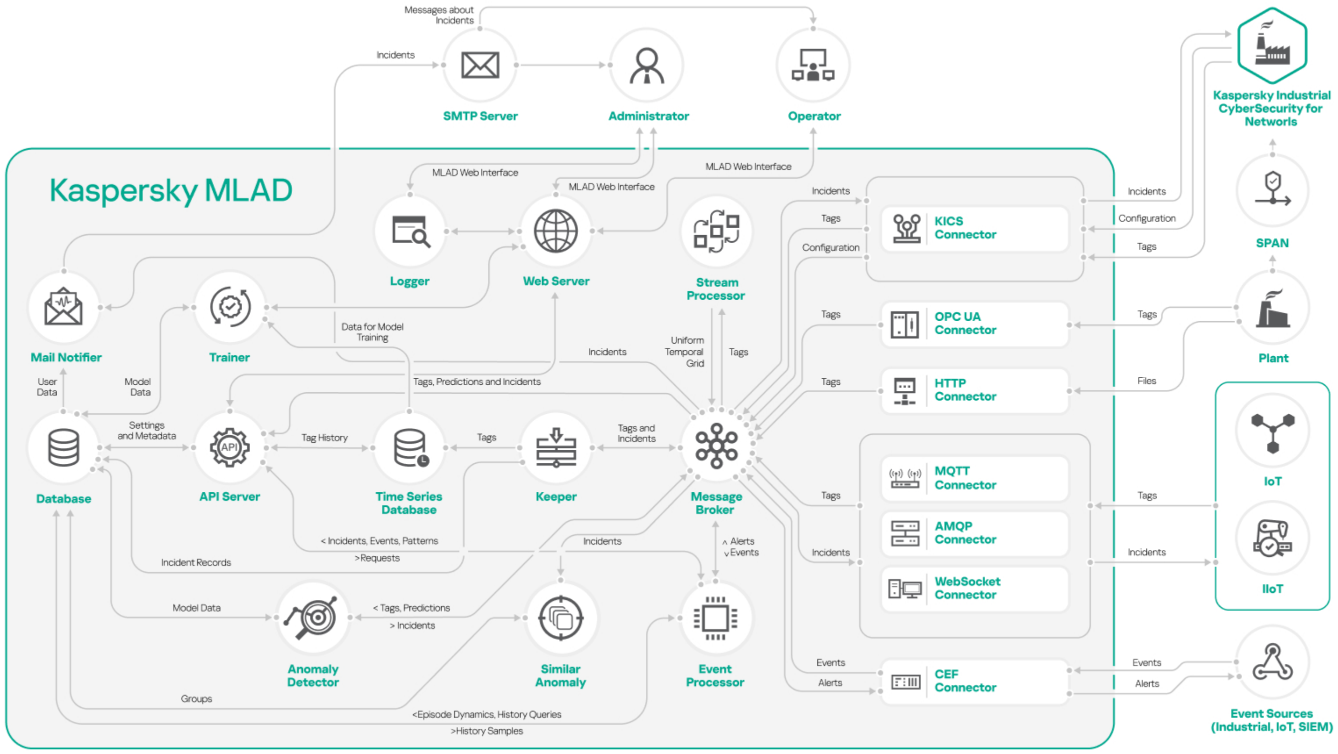


Diagram of interaction between Kaspersky MLAD services

Common deployment scenarios

This section provides a description of the standard scenarios for deploying Kaspersky MLAD in the network of a monitored asset, and provides special considerations when integrating Kaspersky MLAD with other applications.

Kaspersky MLAD supports the following installation options:

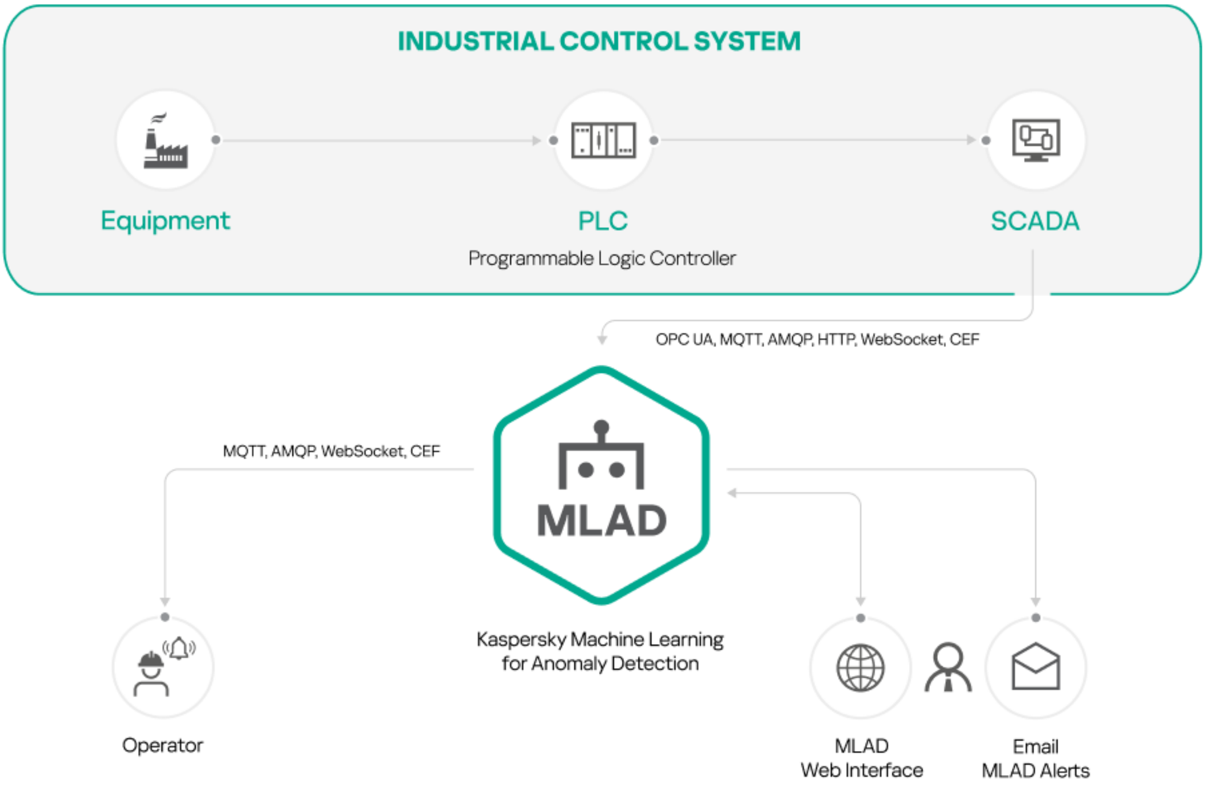
- Standalone installation.
- Installation with Kaspersky Industrial CyberSecurity for Networks version 4.0 and later.

Standalone installation of Kaspersky MLAD

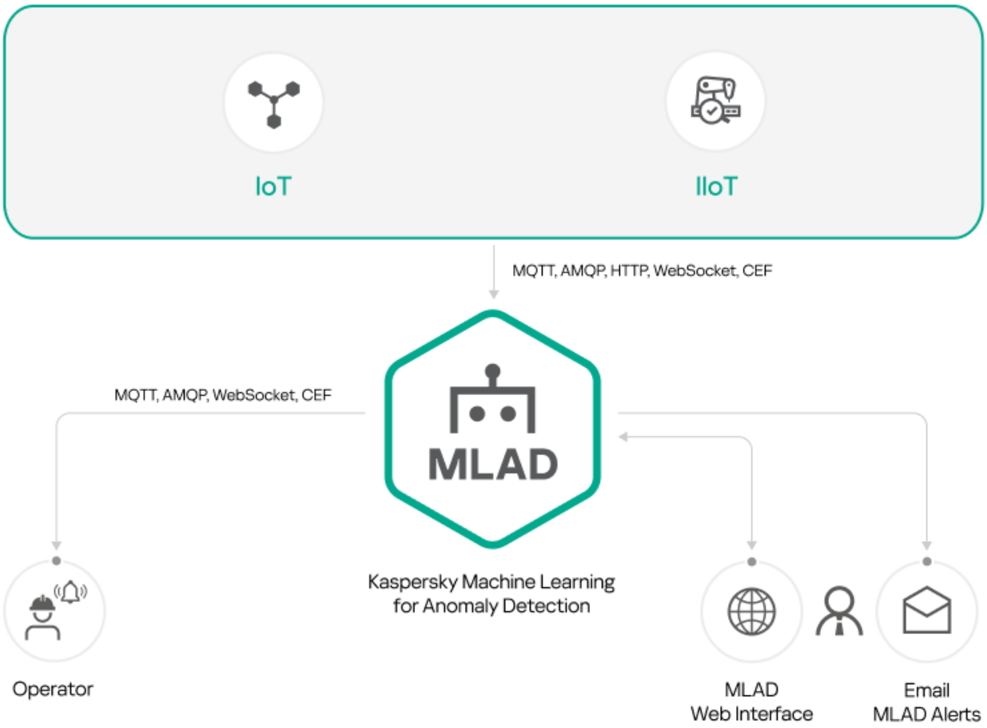
You can install only Kaspersky MLAD if you plan to use the following connectors as a data provider:

- OPC UA Connector
- MQTT Connector
- AMQP Connector
- CEF Connector
- WebSocket Connector
- HTTP Connector

The figures below show example scenarios for standalone installation of Kaspersky MLAD using the connectors described above. You can use any configurations of connectors that are suitable for your monitored asset.


INDUSTRIAL CONTROL SYSTEM
Equipment
PLC
Programmable Logic Controller
SCADA
OPC UA, MQTT, AMQP, HTTP, WebSocket, CEF
MQTT, AMQP, WebSocket, CEF
MLAD
Kaspersky Machine Learning for Anomaly Detection
Operator
MLAD Web Interface
Email MLAD Alerts

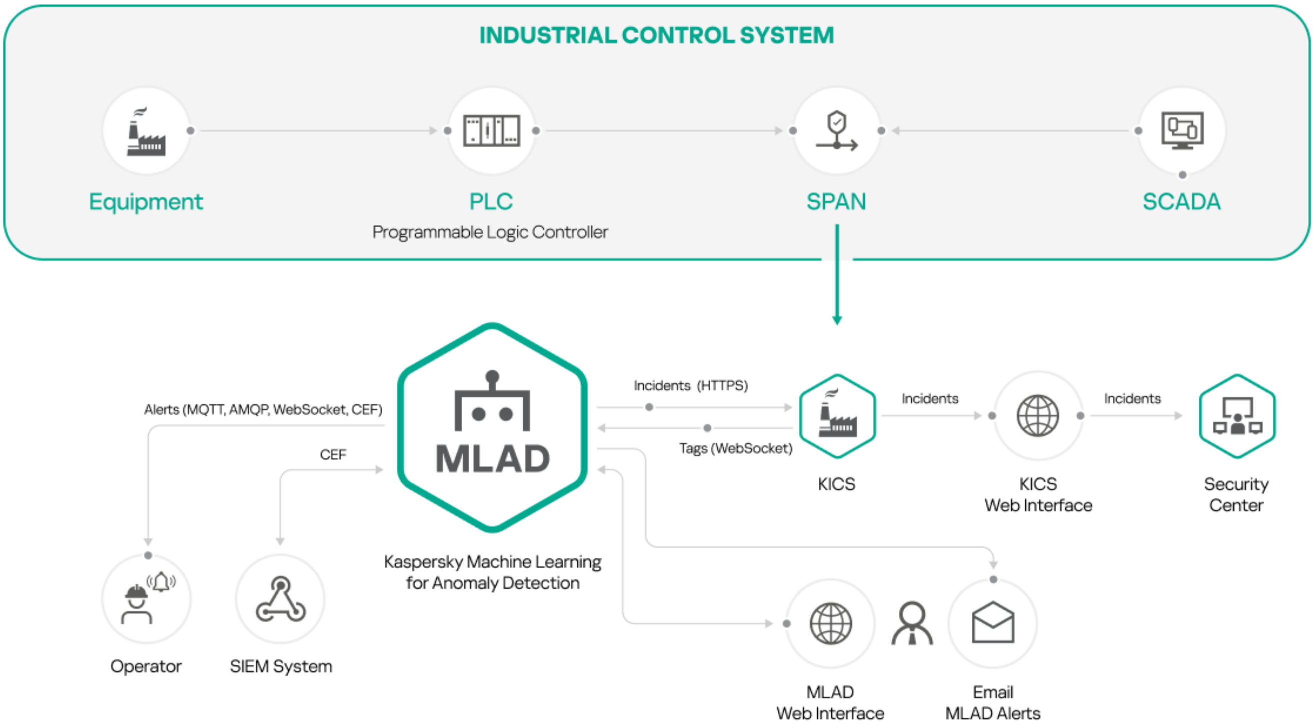
Standalone installation of Kaspersky MLAD using connectors: OPC UA Connector, MQTT Connector, AMQP Connector, HTTP Connector, WebSocket Connector


IoT
IIoT
MQTT, AMQP, HTTP, WebSocket, CEF
MQTT, AMQP, WebSocket, CEF
MLAD
Kaspersky Machine Learning for Anomaly Detection
Operator
MLAD Web Interface
Email MLAD Alerts

Installation of Kaspersky MLAD with Kaspersky Industrial CyberSecurity for Networks

You can install Kaspersky MLAD and Kaspersky Industrial CyberSecurity for Networks if you are planning to use Kaspersky Industrial CyberSecurity for Networks as a data provider (see the figure below).

> Kaspersky Machine Learning for Anomaly Detection is compatible with Kaspersky Industrial CyberSecurity for Networks version 4.0 and later.



Installation of Kaspersky MLAD with Kaspersky Industrial CyberSecurity for Networks

To use this installation option, first install Kaspersky Industrial CyberSecurity for Networks and add a **Generic** connector. Create a communication data package for the added connector and specify the settings for connecting Kaspersky Industrial CyberSecurity for Networks to Kaspersky MLAD. Upload the obtained communication data package to Kaspersky MLAD when configuring the KICS Connector. For detailed information about creating and adding a connector, please refer to the *Adding a connector* section of *Kaspersky Industrial CyberSecurity for Networks Help Guide*.

> Computers with Kaspersky MLAD and Kaspersky Industrial CyberSecurity for Networks installed must belong to the same network.

Telemetry and event data flow diagram

In Kaspersky MLAD, data exchange with the external systems is provided by connectors. To receive telemetry data (tags) and/or events from the external systems, you need to configure the HTTP Connector, MQTT Connector, AMQP Connector, OPC UA Connector, KICS Connector, CEF Connector, and WebSocket Connector.

> If transmission of events and incidents to recipient systems is configured in the application, the application sends registered events and incidents to recipient systems chosen by the system administrator. The application system administrator independently selects the recipient systems and the types of events and incidents to transmit to the recipient systems. The recipient system processes and stores the received data according to its functionality and purpose.

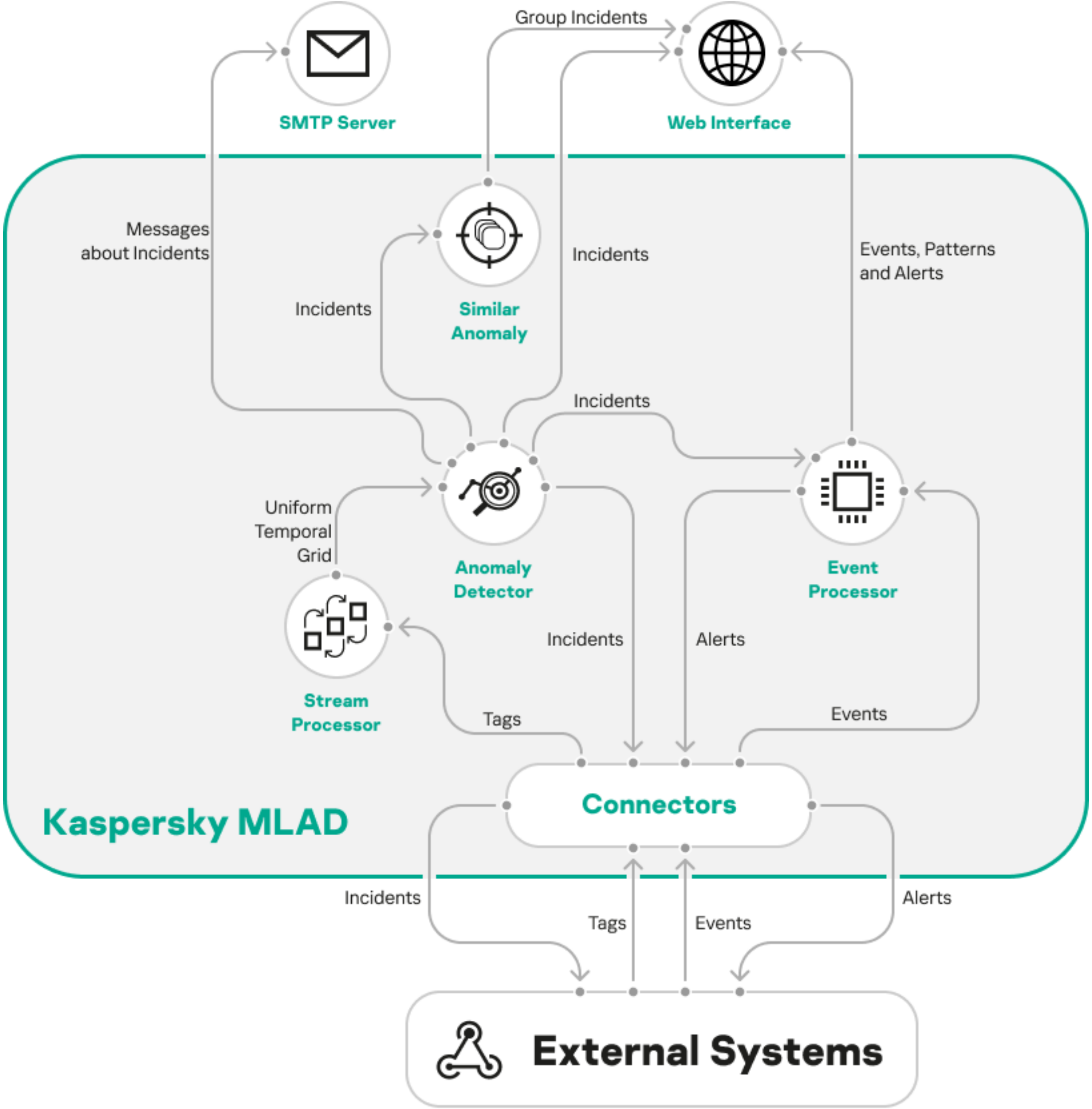
The Stream Processor service performs the initial processing of the telemetry data of the monitored asset, converting the received tags to a uniform temporal grid (UTG). When Stream Processor service detects loss of telemetry data and observations received by Kaspersky MLAD too early or too late, it registers incidents.

The Stream Processor service transfers the UTG-converted data to the ML model of the Anomaly Detector service. If the detectors on which the ML model is based detect deviations from the normal behavior of the monitored asset while processing the received data, the Anomaly Detector service registers incidents. When similar incidents are detected, the Similar Anomaly service generates groups of incidents.

You can view registered incidents and groups of incidents in the **Incidents** section. Kaspersky MLAD also sends incident notifications to the specified email addresses and to external systems using connectors.

Events received by Kaspersky MLAD are processed by the Event Processor service. The Event Processor can also process incidents registered by the Anomaly Detector service. In the stream of events, the Event Processor detects regularities – recurring events and patterns – as well as new events and patterns. When monitors are activated, the Event Processor service sends alerts to external systems about the detection of events, patterns, and event parameter values according to the specified monitoring criteria using the CEF Connector. You can also view information about events, patterns, and monitors in the **Event Processor** section.

The figure below shows the telemetry and event data stream in Kaspersky MLAD.



The telemetry and event data stream in Kaspersky MLAD

Ports used by Kaspersky MLAD

The table below lists the ports that must be opened on the servers where Kaspersky MLAD is installed.

Port	Protocol	Description
443	TCP (HTTPS)	Used to connect to the Kaspersky MLAD web interface.
3001	TCP (HTTPS)	Used to connect to the logging system (Grafana ™).
4999	TCP (HTTP or HTTPS)	Used by the HTTP Connector to download CSV files from external sources.
5518	TCP	Used to connect external event sources to the default CEF Connector. The port number is defined in the .env configuration file.

Installing and removing the application

This section contains step-by-step instructions on installing and removing Kaspersky MLAD.

Installing the application

This section contains a step-by-step description of Kaspersky MLAD installation. During installation, Kaspersky MLAD creates the first application user with the system administrator role.

> Installation of Kaspersky MLAD is performed by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

> Only the software specified in the hardware and software requirements should be installed on the Kaspersky MLAD server.

> Kaspersky MLAD is installed according to the described procedure for application installation. Installation and use of Kaspersky MLAD is possible only on one server. Installation and use of different services and connectors on multiple servers is not possible.

To install Kaspersky MLAD:

1. Unpack the archive named Kaspersky_MLAD_4.0.2.-<build number>_ru-RU_en-US.tar.xz that is included in the distribution kit:

   ```
   tar xf Kaspersky_MLAD_4.0.2.< build number >_ru-RU_en-US.tar.xz
   ```

2. Navigate to the directory named mlad-release-4.0.2-<build number>:

   ```
   cd mlad-release-4.0.2-< build number >
   ```

3. Run the setup.sh installation script:

   ```
   sudo ./setup.sh
   ```

4. Follow the instructions of the Application Setup Wizard.

   Using the Application Setup Wizard, you can change the name and password of the first application user with the system administrator role.

To install Kaspersky MLAD in non-interactive mode:

1. Unpack the archive named Kaspersky_MLAD_4.0.2.-<build number>_ru-RU_en-US.tar.xz that is included in the distribution kit:

   ```
   tar xf Kaspersky_MLAD_4.0.2.< build number >_ru-RU_en-US.tar.xz
   ```

2. Navigate to the directory named mlad-release-4.0.2-<build number>:

   ```
   cd mlad-release-4.0.2-< build number >
   ```

3. Run the setup.sh installation script with the following switches:

   ```
   sudo ./setup.sh -q -e accept
   ```

where:

`-q` means that the application is installed in non-interactive mode. When installing the application in non-interactive mode, Kaspersky MLAD creates the first application user with the system administrator role and assigns it a default user name and password. To obtain the default user name and password, contact a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

`-e accept` means that you accept the terms of the End User License Agreement. You must accept the terms of the End User License Agreement to install the application. If you do not add the `-e accept` switch, installation of the application will not continue.

You can read the text of the End User License Agreement in the text file named license_en.txt located in the 'legal' directory.

The application will be installed on the computer. After installing the application, start it.

Updating the application

This section contains a step-by-step description of the Kaspersky MLAD update procedure.

Updating Kaspersky MLAD is possible starting with application version 4.0.1-001. When Kaspersky MLAD is updated, all of the following data that was uploaded, received, or processed by the previous version of Kaspersky MLAD will be saved: tag configurations, presets, ML models, and settings of Kaspersky MLAD.

Only the software specified in the hardware and software requirements should be installed on the Kaspersky MLAD server.

Kaspersky MLAD is updated to fix security flaws and application vulnerabilities or when new versions of the application are released under the current *Technical Support Agreement*. The application update is performed by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

To update Kaspersky MLAD from the command line:

1. Unpack the archive named mlad-4.0.2-<new build number>.tar.xz that is included in the distribution kit:

   ```
   tar xf mlad-4.0.2-<new build number>.tar.xz
   ```

2. Navigate to the directory where you unpacked Kaspersky MLAD:

   ```
   cd mlad-4.0.2-<new build number>
   ```

3. Run the application update script named upgrade.sh:

   ```
   sudo ./upgrade.sh -u -f <full path to the release.txt file of the application assembly being updated>
   ```

   You can run the upgrade.sh script with the `-h` switch if you want to call up the assistant in the Kaspersky MLAD update interface:

   ```
   sudo ./upgrade.sh -h
   ```

4. Follow the instructions of the Application Upgrade Wizard.

Kaspersky MLAD will be updated to the version specified in the build number. All application files are located in the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<installation build number> by default). A directory named upgrade_backup-4.0.2-<previous build number> will also be created there and will contain a backup copy of the previous version of Kaspersky MLAD.

> You can move the directory containing the backup copy of the application to another storage location in accordance with your company regulations.

Backing up the application

You can back up the application in accordance with your company regulations. Kaspersky MLAD also automatically creates a backup copy when the application is updated.

The application is backed up using the upgrade.sh upgrade script.

> Kaspersky MLAD backup capabilities are available starting with application version 4.0.1-001. The Kaspersky MLAD backup procedure saves all of the following data that was uploaded, received, or processed by Kaspersky MLAD: tag configurations, presets, ML models, and settings of Kaspersky MLAD.

To back up Kaspersky MLAD from the command line:

1. Go to the directory where Kaspersky MLAD is installed:

   ```
   cd mlad-release-4.0.2-< build number >
   ```

2. To back up the application, run the upgrade.sh upgrade script with the `-b` key:

   ```
   sudo ./upgrade.sh -b
   ```

This script creates a directory named backup-4.0.2-<date and time of backup> for storing all application backup files within the Kaspersky MLAD installation directory (mlad-release-4.0.2-<build number> by default).

> You can move the directory containing the backup copy of the application to another storage location in accordance with your company regulations.

Rolling back the application to the previous installed version

This section contains a step-by-step description of the procedure for rolling back the application to the previous installed version using the upgrade.sh script.

> Kaspersky MLAD rollback capabilities are available starting with application version 4.0.1-001.

When rolling back Kaspersky MLAD to the previous installed version, all data received and processed by Kaspersky MLAD from the moment the application was upgraded to the moment of the rollback to the previous version will be lost. You are advised to verify that you have a full backup copy of all Kaspersky MLAD data.

To roll back Kaspersky MLAD to the previous installed version:

1. Go to one of the following directories containing the relevant backup copy of Kaspersky MLAD that the application rollback should restore:

   - upgrade_backup-4.0.2-<build number> – directory storing the application version created automatically during an application upgrade. To go to the directory, run the following command:

     ```
     cd upgrade_backup-4.0.2-<previous build number>
     ```

   - backup-4.0.2-<date and time of backup> – directory storing the application version created when the application was backed up. To go to the directory, run the following command:

     ```
     cd backup-4.0.2-<date and time of backup>
     ```

     When rolling back the application to the previous version, the backup-4.0.2-<date and time of backup> directory must be located in the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<build number> by default).

2. To roll back the application to the previous version, run the application upgrade script named upgrade.sh with the `-r` switch:

   ```
   sudo ./upgrade.sh -r
   ```

3. Follow the instructions of the Application Upgrade Wizard.

Kaspersky MLAD will be rolled back to the previous installed version.

Scenario for restoring Kaspersky MLAD from a backup

If the server hosting Kaspersky MLAD malfunctions, you can restore the application on another server from a backup copy of Kaspersky MLAD using the upgrade.sh script.

The scenario for restoring the application from a backup copy consists of the following steps:

1. **Installing Kaspersky MLAD**

   Install the same version of Kaspersky MLAD that was used for the backup on the server.

2. **Moving a backup copy of the application to the Kaspersky MLAD server**

   Move the directory containing the application backup to the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<installation build number> by default).

3. **Restoring Kaspersky MLAD**

   Go to the directory containing the backup copy of Kaspersky MLAD by running the following command:

   ```
   cd <directory containing the application backup copy>
   ```

To restore the application from a backup copy, run the application upgrade script named upgrade.sh with the `-r` switch:

```
sudo ./upgrade.sh -r
```

Follow the instructions of the Application Upgrade Wizard.

Getting started

Before starting to work with Kaspersky MLAD, you must make sure that the following conditions are fulfilled:

1. The telemetry data source is enabled and configured to send data to Kaspersky MLAD.
2. The data transfer network is prepared to deliver telemetry data from the data source to the Kaspersky MLAD server, the network equipment is properly configured, and data transfer is allowed.
3. Configuration settings and/or configuration files are prepared for the connector that will be used in Kaspersky MLAD to receive telemetry data or events from external systems. The connector must be configured and activated after Kaspersky MLAD is started.
4. Descriptions of tags of received telemetry and assets of the hierarchical structure are prepared as a XLSX file to be imported into Kaspersky MLAD. A description of the presets is supplied in the form of a file in JSON format. The files are created by a qualified technical specialist of the Customer, a Kaspersky specialist or a certified integrator.
5. One or more ML models have been created, trained on historical telemetry data. The ML models are prepared for import into Kaspersky MLAD as TAR files if the files were created by a Kaspersky specialist or a certified integrator within the scope of the *Kaspersky MLAD Model-building and Deployment Service*.
6. The Kaspersky MLAD system administrator has been sent the codes for activating ML models. The ML model activation codes are stored in a secure storage location.

Starting and stopping Kaspersky MLAD

To start the application after it has been stopped:

1. Go to the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<installation build number> by default).
2. In the command line, run the following command:

   ```
   ./mlad-start.sh
   ```

Kaspersky MLAD will be started.

To stop the application:

1. Go to the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<installation build number> by default).
2. In the command line, run the following command:

   ```
   ./mlad-stop.sh
   ```

Kaspersky MLAD will be stopped.

Updating Kaspersky MLAD certificates

The following certificates are used in Kaspersky MLAD:

- Certificates for connecting to Kaspersky MLAD using the web interface.
- Certificates for connecting connectors and services.

It is recommended to update certificates in the following cases:

- Current certificates have been compromised.
- Certificates have expired.
- Certificates need to be updated in accordance with the enterprise information security requirements.

Updating a certificate for connecting to Kaspersky MLAD using the web interface

By default, Kaspersky MLAD uses a self-signed certificate that is automatically generated during the application installation to connect to the web interface. When using a self-signed certificate to connect to the Kaspersky MLAD web interface, the browser displays a warning that the security certificate or the established connection is not trusted.

To use trusted certificates to connect to the Kaspersky MLAD web interface, you can replace the self-signed certificate with a certificate received from a recognized certification authority or with a custom certificate that complies with the security standards of your organization.

By default, Kaspersky MLAD uses the mlad-4.0.2-<installation build number>/ssl/nginx/ directory to store certificates for connecting to the web interface.

> The certificate for connecting to Kaspersky MLAD using the web interface can be updated by a qualified technical specialist of the Customer, a Kaspersky employee or a certified integrator.

To update certificates for connecting to Kaspersky MLAD using the web interface:

1. Obtain a trusted certificate and a key for this certificate to connect to the Kaspersky MLAD web interface.

   A certificate must be received for the IP address and domain name of the server on which Kaspersky MLAD is installed.

2. Go to the directory containing the trusted certificate and the key to this certificate.

3. In the command line, run the following commands:

   ```
   sudo chown root:root <new certificate.crt> <new certificate key.key>
   sudo chmod 640 <new certificate.crt> <new certificate key.key>
   sudo cp <new certificate.crt> mlad-4.0.2-<installation build
   number>/ssl/nginx/mlad_nginx.crt
   sudo cp <new certificate key.key> mlad-4.0.2-<installation build
   number>/ssl/nginx/mlad_nginx.key
   ```

The new certificate and its key are saved in the mlad-4.0.2-<installation build number>/ssl/nginx/ directory as the mlad_nginx.crt and mlad_nginx.key files, respectively.

4. Restart Kaspersky MLAD by executing the following commands in the command line:

```
mlad-4.0.2-<installation build number>/mlad-stop.sh
mlad-4.0.2-<installation build number>/mlad-start.sh
```

After restarting, Kaspersky MLAD uses the new certificate to connect to the web interface.

Updating a certificate for connecting connectors and services

In Kaspersky MLAD, you can use a secure connection for MQTT Connector, AMQP Connector, WebSocket Connector, and the Mail Notifier service. You can update certificates for connecting these connectors and the Mail Notifier service using a secure connection in the **System parameters** section of the administrator menu.

> To connect the MQTT Connector, AMQP Connector, and WebSocket Connector as well as the Mail Notifier service over a secure connection, it is recommended to use certificates created according to the X.509 standard with a certificate key length of at least 4,096 bits.

The certificate for connecting the KICS Connector is contained in the communication data package, which you can update in Kaspersky Industrial CyberSecurity for Networks. You can upload the updated communication data package to Kaspersky MLAD when configuring the KICS Connector. For detailed information about creating a communication data package, please refer to the *Kaspersky Industrial CyberSecurity for Networks Help Guide*.

> Kaspersky Machine Learning for Anomaly Detection is compatible with Kaspersky Industrial CyberSecurity for Networks version 4.0 and later.

First startup of Kaspersky MLAD

This section describes the sequence of application configuration steps that must be performed by the system administrator when Kaspersky MLAD is started for the first time.

The first startup of Kaspersky MLAD consists of the following steps:

1. **Starting Kaspersky MLAD**

   Start Kaspersky MLAD. The following services required for Kaspersky MLAD operation will be started:

   - API Server.
   - Web Server.
   - Message Broker.
   - Keeper.
   - Time Series Database.
   - Database.

- Logger

2. **Connecting to the Kaspersky MLAD web interface**

   Open the application web interface in a supported browser and enter the user name and password of the first Kaspersky MLAD user with the system administrator role defined during installation of the application. Change the password for your user account. For a secure connection to Kaspersky MLAD web interface, install a trusted certificate.

3. **Configuring services**

   In the **System parameters** section of the administrator menu, configure the services that you need to use for your monitored asset. In the **Services** section, check the statuses of the services and start them, if necessary. For example, the *Anomaly Detector* service must be running for correct anomaly detection.

4. **Uploading a configuration of tags and assets of the hierarchical structure to Kaspersky MLAD and creating presets**

   Configuration of tags, assets and presets is created by a Kaspersky expert or integrator while deploying the application and building an ML model. Tag and asset configuration is described in a XLSX file. A preset configuration is described in a JSON file. For examples of descriptions of the configuration of tags and assets, as well as preset configuration, see the Appendix.

   For subsequent operation, upload tag and asset configuration to Kaspersky MLAD. Download preset configuration or create new presets from tags.

5. **Uploading and creating ML models**

   An ML model is not included in the application distribution kit but is provided as part of the *Kaspersky MLAD Model-building and Deployment Service*.

   Download the ML model, if it was provided as part of the *Kaspersky MLAD Model-building and Deployment Service*, or create it yourself using the Model Builder. Activate the downloaded ML model. To activate the ML model, you must enter a model activation code.

6. **Configuring connectors**

   To work with data, configure the connectors used at your monitored asset. You can configure the following connectors:

   - KICS Connector.
   - OPC UA Connector.
   - CEF Connector.
   - HTTP Connector.
   - MQTT Connector.
   - AMQP Connector.
   - WebSocket Connector.

7. **Connecting to a data source**

   When the above connectors are configured, start the connectors used for your monitored asset. Go to the **Dashboard** section and make sure that data is being received by Kaspersky MLAD in online mode.

8. **Configure attention**

To work with events and patterns, configure attention settings and display of event parameters. The Event Processor service detects events and patterns only for the attention directions defined in the attention settings.

9. **Creating user accounts**

   Create accounts for users of the application and assign the necessary roles to them. Configure incident notifications for users.

Kaspersky Machine Learning for Anomaly Detection is prepared for operation, and the application is receiving and processing data.

Users can start working with Kaspersky MLAD using the web interface.

Removing the application

Removal of Kaspersky MLAD must be performed by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

When Kaspersky MLAD is removed, all Kaspersky MLAD data that was received, uploaded, and processed since the application was installed will be lost. You are advised to verify that you have a full backup copy of all Kaspersky MLAD data. When you update the application, Kaspersky MLAD automatically creates a backup copy of the previous application version. You can also manually back up the application.

To remove Kaspersky MLAD:

1. Go to the directory where Kaspersky MLAD is installed (mlad-release-4.0.2-<installation build number> by default):

   ```
   cd mlad-release-4.0.2-< build number >
   ```

2. Run the setup.sh installation script with the -u switch:

   ```
   sudo ./setup.sh -u
   ```

3. Confirm removal of Kaspersky MLAD services.

Kaspersky MLAD will be removed.

Kaspersky MLAD web interface

Kaspersky MLAD is managed through a web interface. This section provides a description of the main elements of the Kaspersky MLAD web interface.

The main window of the application web interface contains the following items:

- Main menu in the left part of the application web interface window.
- Workspace in the central part of the application web interface window.

Sections of the main menu are available to users with access rights to the corresponding functions of the application. Access to application functions is determined by the list of rights assigned to the user role.

System administrators can access a menu that provides the capability to configure application settings, manage user accounts, configure incident notifications, manage tags, and proceed to the logging system page to view logs.

At the bottom of the main menu and the administrator menu, the user menu is available, which provides the opportunity to select the language of the web interface, change the password for your account, log out of your account, and navigate between the menus. To switch between the main menu and the administrator menu, click one of the following buttons:

- ☰ – to navigate to the administrator menu.
- ⊞ – to navigate to the main menu.

If necessary, you can collapse or expand the menu by clicking « or », respectively, in the upper-left corner of the page.

Main menu

The table below describes the sections of the main menu of Kaspersky MLAD.

Main menu sections

Section	Description
⊞ Dashboard	Opens the section containing information about the latest incidents, services and their statuses.
🖥 Monitoring	Opens the section that displays data received by the system in real time. You can also configure the settings for displaying incoming data on a graph.
🕓 History	Opens the section that contains a complete history of data received by the system and the results of its analysis by ML models. You can also configure the settings for displaying historical data on the graph.
[□] Time slice	Opens the section containing information about the values of process parameters received from sensors at the same point in time. You can also configure the settings for displaying the data on the graph.
🔍 Event Processor	Opens the section where you can view information about events received from external systems and patterns detected for them, as well as manage monitors to track specific events, patterns, or event parameter values.
🚨 Incidents	Opens the section that contains the log of detected incidents. As part of the incident analysis, you can also add a status, reason, expert opinion, and comments to an incident or an incident group.

Models	Opens the section enabling you to view information about ML models and ML model templates used in the system, as well as to manage them. ML models and ML model templates can be managed only by system administrators.
Presets	Opens the section enabling you to view information about available presets, edit the preset settings, and create presets.
Services	Opens the section enabling you to view information about services and their statuses, as well as to start, stop, and restart services. Service status management is available only to system administrators.

Administrator menu

The table below describes the sections of the Kaspersky MLAD administrator menu.

Administrator menu sections

Section	Description
Users	Opens the section in which you can manage user accounts.
Roles	Opens the section containing information about available user roles.
Rights	Opens the section containing information about the permissions of users.
Notifications	Opens the section where you can manage notifications that the application sends to the users when incidents are registered.
System parameters	Opens the section in which you can manage the settings of Kaspersky MLAD services.
Assets	Opens the section in which you can manage tags.

User menu

The table below describes the elements of the Kaspersky MLAD user menu.

User menu elements

Menu element	Description
⚐	Lets you select the localization language for the Kaspersky MLAD web interface. It is available in English and Russian.
🕮	Opens the Kaspersky MLAD Help Guide in a new browser tab.
ⓘ	Opens the page containing brief information about the application.
🗎	Takes you to the logging system (Grafana ™) in a new browser tab. This section is available only to system administrators.
☰	Navigates to the administrator menu from the main menu. In the administrator menu you can manage user account credentials, view user roles and permissions, configure incident notifications, and manage tags. The administrator menu is available only to system administrators.
⊞	Navigates to the main menu from the administrator menu. In the main menu, you can view historical and real-time data, view logged incidents, events and patterns, and view information about the created ML models.
@	Allows you to change the password for the current user account and log out of the account.

Connecting to Kaspersky MLAD and terminating a user session

Use a supported browser to connect to Kaspersky MLAD web interface.

When a user connects to the Kaspersky MLAD web interface, the application generates a token whose validity time determines the maximum duration of an inactive user session. While Kaspersky MLAD is being actively used, the application does not prompt for user account credentials as long as the connection is being used by the same computer, browser, and user account. A user session is considered active in the following cases:

- The user interacts with elements of the application interface (for example, clicks buttons or navigates to sections of the application menu).
- The user enters parameter values using the keyboard.

If an authorized user does not use the application for a time period exceeding the **User inactivity period (min)**, Kaspersky MLAD automatically terminates the connection session for this user. To terminate a connection session before the token expires, an authorized user can manually sign out of their user account.

If necessary, the system administrator can revoke authentication tokens for a user account. When a token is revoked for a user, their work sessions in the application are terminated simultaneously on all devices where they are authorized.

> The web address, user name and password for signing in to the application must be requested from the Kaspersky MLAD system administrator.

Connecting to the web interface

To connect to Kaspersky MLAD using a browser:

1. Open a supported browser on your computer.
2. In the browser address bar, enter the Kaspersky MLAD server web address received from the Kaspersky MLAD system administrator.
3. On the account credential entry page that opens, enter your user name and password.

   If you are connecting to the web interface for the first time, use the user name and password of the first user with the system administrator role specified during installation of the application.
4. Click the **Sign in** button or press **ENTER**.

   The **Dashboard** opens in the browser window.

   When connecting to Kaspersky MLAD for the first time, the **password change window** opens in the browser. If the password change was made optional in the security settings, you can skip changing the password by clicking the **Skip** button and change it later.

- **New password** – new password for the user account.

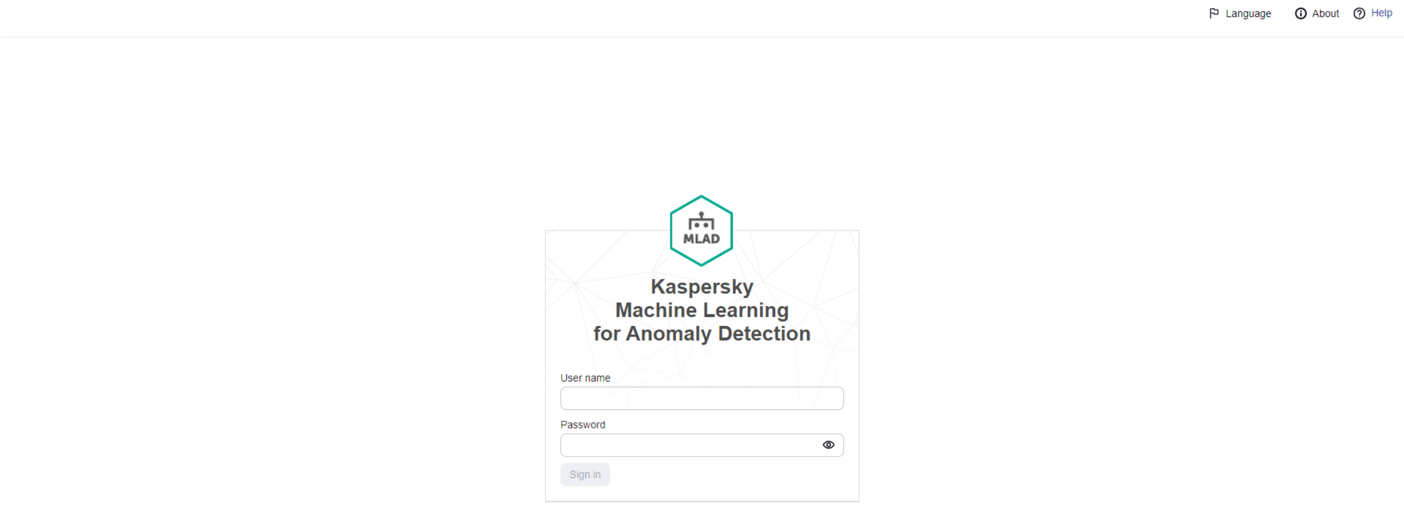
  The new password must meet the following requirements:

  - Must not match previously used passwords. The specific number of most recently used passwords that must not be reused is defined by the user with the system administrator role.
  - Must contain the minimum number of characters defined by the administrator when configuring the security settings.
  - Must contain letters of the English alphabet, numerals and/or special characters in accordance with the password policy that was set by the administrator when configuring the security settings.
- **Confirm password** means you must type the password again to confirm the password for the user account.

The change password window also opens in your browser upon expiration of the password that was set when configuring the security settings.

If you close the browser window without terminating the connection session, the session remains active until the time limit that was set when configuring the security settings. During this time, the application continues to grant access to the Kaspersky MLAD web interface without prompting for user account credentials, provided that the connection is used by the same computer, browser, and operating system user account. If the application user is inactive for longer than the time limit that was specified in the security settings, Kaspersky MLAD terminates the user session.

In case of unsuccessful authorization attempts, Kaspersky MLAD will block your account when the maximum number of unsuccessful authorization attempts is reached for a certain period. The maximum number of unsuccessful authorization attempts and the account blocking period are set when configuring the security settings of Kaspersky MLAD.



Page for entering the account credentials for Kaspersky MLAD

Terminating a Kaspersky MLAD connection session

When you are done working with Kaspersky MLAD in a browser, you must terminate the connection session.

To terminate the application connection session:

- in the browser window, in the lower-left corner of the Kaspersky MLAD web interface, click the button 👤 and select **Sign out of Kaspersky MLAD**.

After the application connection session is terminated, the browser window shows the page for entering account credentials.

Changing a user account password

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

- You are connecting to Kaspersky MLAD for the first time after the user account was created in the application.
- The current password has been compromised.
- The password is expiring in accordance with the information security requirements at the enterprise.

To change the password of your own user account:

1. In the lower-left corner of the Kaspersky MLAD web interface page, click the button 👤 and select **Change password**.

   The **Change password** window opens in the browser.

2. In the **Current password** field, enter your current password.

3. In the **New password** and **Confirm password** fields, enter the new password.

   The new password must meet the following requirements:

   - Must not match previously used passwords. The specific number of most recently used passwords that must not be reused is defined in the administrator menu.
   - Must contain the minimum number of characters defined when configuring the security settings.
   - Must contain letters of the English alphabet, numerals and/or special characters in accordance with the password policy that was set when configuring the security settings.

4. Click the **Edit** button.

Selecting the localization language for the Kaspersky MLAD web interface

Kaspersky MLAD provides the option to use English or Russian for the application web interface.

To change the localization language of the application web interface:

1. In the lower-left corner of the Kaspersky MLAD web interface page, click the **Language** button.

2. Select the required localization language: Russian or English.

Licensing the application

This section provides information about general concepts related to licensing of Kaspersky MLAD.

About the End User License Agreement

The *End User License Agreement* (EULA) is a binding agreement between you and AO Kaspersky Lab that stipulates the terms on which you may use the application.

Please carefully read the terms of the End User License Agreement before using the application.

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

- During installation and update of Kaspersky MLAD.
- By reading the license_en.txt file. This file is included in the application distribution kit.

You accept the terms of the End User License Agreement when you confirm your consent to the End User License Agreement during the installation or update of the application. If you do not accept the terms of the End User License Agreement, please stop the installation or update of the application and do not use the application.

About the license

A *license* is a time-limited right to use the application as granted under the End User License Agreement.

The license includes the right to use the application in accordance with the terms of the License Agreement, as well as to receive technical support. The term of use of the application depends on the type of license under which the application was purchased.

The following types of licenses are available:

- Base: To use the application functionality when purchasing Kaspersky MLAD for the first time.
- Renewal: To use the application functionality upon repeated purchase of Kaspersky MLAD.

Each license type can be unlimited or limited in time to 1, 2, or 3 years. When purchasing a license for a specific term, it is recommended to renew the license after its expiration date.

Technical support services are provided if you have an active *Technical Support Agreement*. The scope of provided technical support services is determined by the current *Technical Support Agreement*.

About the license certificate

The *license certificate* is a document that is handed over to you along with the key file.

The license certificate contains the following information about the license provided:

- License key or order number
- Information about the user who is granted the license
- Information about the application that can be activated under the provided license
- Limitation on the number of licensing units (for example, tags by which the application can receive telemetry data)
- Start date of the license term
- License expiration date or license term
- License type

Processing and storing data in Kaspersky MLAD

This section contains information about data provision and directories for storing data.

About data provision

The application does not transfer users' personal data to Kaspersky. Users' personal data is processed locally on the computers where the application is installed.

Data transferred to external systems

If sending email notifications about incident logging is enabled, the application transfers the following data to the SMTP server:

- Date and time of the logging of the incident
- Name of the ML model that logged the incident
- Top tag name
- Top tag description
- Top tag value at the time the incident is logged
- Top tag measurement units
- Link to the **History** section at the time of the start of the incident
- Incident ID
- Name of the detector that logged the incident
- Cumulative mean square error (MSE) value at the time the incident was logged
- Blocking threshold value exceeded at the time the incident was logged.

If sending notifications about incident logging through the MQTT Connector, AMQP Connector, WebSocket Connector, and/or KICS Connector is enabled, the application transfers the following data to the MQTT broker, AMQP broker, WebSocket server, and/or to Kaspersky Industrial CyberSecurity for Networks:

- Incident ID
- Date and time of the logging of the incident
- Date and time of the incident completion
- Name and unique ID (UUID) of the ML model that logged the incident
- Unique ID (UUID) of the ML model element
- Top tag ID and description

- Name of the detector that logged the incident
- Link to the **History** section at the time of the start of the incident
- Cumulative mean square error (MSE) value at the time the incident is logged (if any)
- Blocking threshold value exceeded at the time the incident is logged (if any)
- Top tag value at the time the incident is logged
- Incident status
- Incident comment (if any)
- Incident group ID (if any)
- Incident group name (if any)
- Expert opinion (if any)
- IDs of the relevant tags
- Reason for the incident (if any).

If notifications about the logged incidents are configured to be sent via the CEF connector, the application transfers the following data to the SIEM system:

- Application vendor name
- Application name
- Kaspersky MLAD version
- Application signature ID
- Date and time of the logging of the incident
- Date and time of the incident completion
- Name of the detector that logged the incident
- Name of the ML model that logged the incident
- Link to the **History** section at the time of the start of the incident
- Top tag description
- Incident comment (if any)
- Incident group name (if any)
- Top tag value at the time the incident is logged
- Incident group ID (if any)
- Incident ID

- Top tag ID.

If the logged events are configured to be sent via the CEF connector, the application transfers the following data to the SIEM system:

- Application vendor name
- Application name
- Kaspersky MLAD version
- Application signature ID
- Name of the monitor that logged the event
- Monitor ID
- Date and time when the event was logged
- Number of activations on the sliding window
- Type of the element that caused the monitor activation
- Information on whether the registered event is new to the application
- Last events or patterns that activated the monitor
- Condition for the monitor filters
- Information on whether the monitor is activated only by new events or patterns.

If sending information security event logs is enabled, the application transfers the following data to the Syslog server:

- Application vendor name
- Application name
- Kaspersky MLAD version
- Application signature ID
- ID of the information security event
- Date and time when the information security event occurred
- Information security event type
- Information security event subtype
- Information security event severity level
- Name of the user whose actions resulted in the information security event entry
- IP address of the computer from which the user performed the actions logged into the information security event log

- Information security event outcome
- Brief summary of the information security event
- Detailed description of the information security event.

Data processed locally on the Kaspersky MLAD server

To perform its main functions the application can receive, store and process the following information:

- Information about the full backup copies of the application, if the application has been backed up or updated. The Kaspersky MLAD server stores information about full application backups until they are deleted by the user.
- Information about the backup copies of the Docker **volumes** that are created during uninstallation of the application. The Kaspersky MLAD server stores information about Docker volume backups until they are deleted by the user.
- Files containing the text of the End User License Agreement of the currently installed application version.
- Certificates for connecting to the application using the web interface.
- Certificates and certificate keys for encrypting the connection between Kaspersky MLAD connectors and services and the external systems.
- Public keys for verifying the digital signature of the distribution package. The Kaspersky MLAD server stores public keys until they are deleted by the user.
- User account data: account ID, last name, first name, middle name, email address, account status (active or blocked), password.

  Values that do not personally identify the user (for example, shop and job title) can be entered in place of the last name, first name and middle name of a user. The information specified in the **Last name**, **First name** and **Middle name** fields for users when creating user accounts is stored in plain text and is not processed by the application.

  The email addresses that are specified when creating accounts are used for the user names when users connect to the web interface of the application. User names are indicated in the information security event logs. Email addresses are used to send notifications about registered incidents.

  Users' email addresses are stored in plain text.

  Kaspersky MLAD does not store user passwords in plain text. The scrypt hash sum calculation algorithm is used to store passwords. Kaspersky MLAD adds salt to the password to prevent decoding. User passwords are not written to application logs.

  The system administrator enters information about user accounts in the administrator menu.
- Data about roles and the rights assigned to these roles: role ID, role name, role status (active or inactive), list of assigned rights, date and time of role creation, date and time of role modification.

  The system administrator enters information about roles in the administrator menu.
- Data about incident notifications: notification ID, email address for sending the notification, incident type, user to whom the notification is sent, notification status (active or inactive).

  The system administrator enters information about notifications in the administrator menu.
- Data about Kaspersky MLAD settings:

- Main application settings: monitored asset name, application web address, IP address for connecting to the program, interval for receiving data from the Message Broker service, interval for receiving statistical data about incidents from the database, monitored asset time zone.

- Application security settings: number of authorization attempts, user blocking period, user inactivity period, information on whether the password must be changed upon the first connection, number of user passwords stored in the history, password validity period, minimum password length, information on whether uppercase, lowercase Latin letters, numbers and/or special characters (_! @ # $% ^ & *) must be used in the password, size and storage time of the information security event logs.

- Anomaly Detector settings: information on whether to use the Limit Detector, Forecaster, XGBoost, and/or Rule Detector, information on whether to skip data gaps, the maximum number of records requested from the Message Broker service, the number of messages sent in one block to the Message Broker, the number of simultaneously running ML models.

- Keeper settings: information on whether all tags must be stored, waiting time to receive tags, incidents, and metrics.

- Mail Notifier settings: SMTP server address and port, user name and password for connecting to the SMTP server, information on whether to use a TLS connection, SMTP server certificate and certificate key.

- Similar Anomaly settings: minimum and maximum number of incidents for the group, maximum interval between similar incidents.

- Stream Processor settings: frequency of the uniform sequence, configuration file with Stream Processor settings.

  The Stream Processor configuration file stores the IDs of the tags processed by the service and the values of tag processing settings.

  > The values of the tag processing settings are set by Kaspersky experts individually for each monitored asset.

- HTTP Connector settings: information on whether to write data to the Message Broker, information on whether to save the received file, the size of the block to be written, the maximum size of the uploaded file.

- MQTT Connector settings: information on whether to use a TLS connection, address and port of the MQTT broker, user name and password to connect to the MQTT broker, root certificate, client application certificate and key to the client application certificate, list of MQTT subscriptions to receive tags, MQTT topic for publishing messages, format for processing incoming data, connector configuration file, information on whether to scale the received tag values.

  The MQTT Connector configuration file stores IDs, names, descriptions, types, and measurement units for tags.

- AMQP Connector settings: information on whether to use a TLS connection, address and port of the AMQP broker, user name and password to connect to the AMQP broker, root certificate, client application certificate and key to the client application certificate, AMQP virtual node, names of AMQP exchange points for receiving tags and publishing messages, AMQP topic for publishing messages, format for processing incoming data, connector configuration file, information on whether to scale the received tag values.

  The AMQP Connector configuration file stores IDs, names, descriptions, types, and measurement units for tags.

- OPC UA Connector settings: connection point name, OPC UA server connection timeout, connector configuration file, historical data interval, start and end of the historical data period, size of the historical data block sent by the OPC UA server, size of the historical data block sent to Message Broker.

  - KICS Connector settings: communication data package for the KICS Connector, password for the KICS Connector, information on whether to send messages to Kaspersky Industrial CyberSecurity for Networks, the tag sampling frequency, information on whether to scale the received tag values.

  - CEF Connector settings: information on whether to receive events for the Event Processor, information on whether to send registered incidents and/or events to the SIEM system, the IP address and port for sending events and incidents to SIEM systems, information on whether to send the information security event logs to the Syslog server, the transport protocol for sending information security events to the Syslog server, the address and port of the Syslog server for sending information security events.

  - WebSocket Connector settings: WebSocket server web address, root certificate, client application certificate and client application certificate key, incoming data processing format, connector configuration file, information on whether to scale the received tag values, information on whether to send incidents.

  - Event Processor settings: service configuration file, information on whether to process incidents as events, the maximum number of network layers, the coefficient defining the permitted dispersion of the pattern duration, the interval for receiving epoch events, the epoch size in online mode, the mechanism for saving the Event Processor status, component backup frequency, the backup copy of the Event Processor status, epoch size in sleep mode, alert mode when the monitor is activated in sleep mode, sleep mode frequency and duration, event history interval for processing in sleep mode.

  - Incident status settings: incident status ID, incident status names in Russian and English, sorting sequence number, information on whether to display the registered incidents with this status.

  - Incident cause settings: incident cause ID, incident cause name, sorting sequence number.

  - Logging service settings: logging levels of the services and application connectors.

  - Settings of the time intervals for charts in the **Monitoring**, **History**, and **Time slice** sections: time interval ID, time interval name in Russian and English, sorting sequence number, ID of the user who created the time interval, ID of the user who last changed the time interval, time interval value.

  - Settings for displaying the items of the main menu and administrator menu: information on whether to display the items of the main menu and administrator menu in the application web interface.

  The system administrator defines Kaspersky MLAD settings in the administrator menu.

- Asset and tag data: asset name, asset ID, asset icon, parent asset ID, asset description and type, asset type ID and name, asset type custom parameters names and values, asset type description, tag ID and name, tag alternative name, tag icon, tag description, tag type, tag measurement unit, upper and lower thresholds for blocking, signaling, and measurement confidence, upper and lower limits for displaying tags, an expression by which the tag value must be calculated based on the value transmitted to the application, tag comment, location coordinates of the monitored asset sensor along the abscissa, ordinate, and applicate axes, the name of the device from which the tags are received from the external system, the color of the additional threshold lines.

  The system administrator enters information about assets and tags in the administrator menu.

- Preset data: preset name, preset ID, preset icon, names and IDs of the tags included in the preset, information on whether to configure an expression for the **Time slice** section, labels on the abscissa and ordinate axes, the name of the expression for calculating tag values, expressions for calculating the tag values, the color of the chart for the preset in the **Time slice** section.

  Any user can enter data in the **Presets** section.

- Information about the number of tags and events received per second. The application calculates the data based on the data received from external systems.

- Information about the values of tags and events received by the system. Data is received from external systems for which data receipt is configured.
- Information about predicted tag values, cumulative mean square error (MSE), and individual tag error. The application calculates the data based on the data received from external systems.
- Information about the application service statuses: the name and current status of the service. The application displays the service status derived from the corresponding components.
- Data on registered incidents and groups of incidents: incident ID, date and time when the incident was registered, top tag name and ID, incident cause, name of the detector that registered the incident, incident group name, incident status, ML model name, ML model branch, cumulative mean square error (MSE) value, cumulative mean square error (MSE) threshold value, top tag value, blocking thresholds, tag description and measurement units, incident type, date and time when the observation was generated, time by which observation generation is ahead or behind the receipt of this observation by the application, an expert opinion on the incident and on the group, incident comment, incident group name and ID, the number of incidents in the group, the date and time when the incident group was created, the status of the registered incidents in the group, IDs of the relevant tags, blocking threshold reached when the incident was registered.

  The application generates this data as a result of analysis of the received data and on the basis of the settings specified by the user.
- Settings for displaying charts in the **Monitoring** and **History** sections: chart height, preset for going to the **History** section (only when configuring the chart display settings in the **Monitoring** section), information on whether to display the observation chart with the selected color, the observation chart color, information on whether to display the prediction chart with the selected color, prediction chart color, information on whether to display the names and descriptions of tags on the charts, the predicted value of the tag and/or a personal tag error, information on whether to display indicators for all incidents on the charts, information on whether to display blocking thresholds and/or additional threshold lines on the charts, ML model branch used to generate predicted values, presets, time intervals, date and time for displaying charts.

  Any user can enter data in the **Monitoring** and **History** sections.
- Chart display settings in the **Time slice** section: chart height, ML model branch used to generate predicted values, presets, time intervals, date and time for displaying charts.

  Any user can enter data in the **Time slice** section.
- Settings for processing and displaying data for the event processor: events parameters used to register patterns (individual for each monitored asset), information on whether to register patterns by a template (regular expression), template settings (individual for each monitored asset).

  If the **Process incidents as events** option is enabled in the Event Processor settings, the application stores and processes the following data:

  - Name of the detector
  - Name of the ML model being used
  - Top tag name and ID
  - Name of the incident group to which the registered incident belongs
  - Top tag value
  - Incident ID.

  Any user can enter the event processor data in the **Event Processor** section.

- Data on events and patterns monitoring in the event processor: monitor name and ID, the number of registered activations based on the sliding window, date and time of the last activation, the type of element that caused the monitor activation, the setting determining what is monitored, sliding window, threshold, names of event parameters which values are monitored, monitored types of values, event parameters on which the model is focused, monitored event parameter values, stack (list of monitor activations arranged by time) limit, ID of the event parameter value that caused the monitor activation, ID of the event detection of which caused the monitor activation, the ID of the pattern detection of which caused the monitor activation, date and time when the event was detected in the event stream, the time interval between the current event and the previous event in the event flow determined by a sliding window, the number of event repetitions in the event flow determined by a sliding window, the date and time of the last event detection in the event flow determined by a sliding window, the parameter values of the event received by the monitored asset, the number of events included in the pattern that caused the monitor activation.

  The application generates data by analyzing the received data and the settings specified in the **Event Processor** section.

- Data on registration of patterns in the event processor: pattern ID, date and time of the last pattern detection in the interval, the number of pattern detections in the event flow of the monitored asset during the specified period, the number of events n the pattern, date and time of the last pattern detection in the event flow or in sleep mode, date and time of the beginning and end of the pattern loading period, pattern type, attention direction, event parameter value, information on whether to register patterns based on a template (regular expression), template parameters (individual for each monitored asset), the time interval between the selected pattern and pattern detected in the sequence of patterns on the current layer before the selected pattern, the total number of activations, the pattern end date and time in the sequence of patterns on the current layer, the pattern layer number, IDs of events included in the pattern, the date and time when the event was detected in the pattern structure, the number of event parameters for which the values are received from the monitored asset.

  The application generates data by analyzing the data and the settings specified in the **Event Processor** section.

- Information about ML models and their parameters: ID and unique ID (UUID) of the ML model, name, description, status and state of the ML model, name of the user who last modified the ML model, date and time when the ML model was last modified, name of the user who created the ML model, date and time when the ML model was created or loaded, the names and IDs of its elements, the time interval, and markup for the inference.

  A system administrator or a user with the **Manage ML models** rights set in the **Models** section can enter and/or upload the data.

- Information about the ML model elements and their parameters:

  - Parameters common for all types of ML model elements: ID, name and description of the ML model element, the time interval after which a repeated incident is generated, the time interval during which repeated incidents are not registered, the grid step in seconds, the incident cause and status, color of the incident indicator points, expert opinion.

  - Main parameters of ML model neural network elements: element architecture, names and IDs of the input tags, names and IDs of the output tags, incident registration threshold, cumulative mean square error (MSE) power, cumulative mean square error (MSE) smoothing degree, the number of steps in the input window for the input values, the number of steps by which the beginning of the output window is shifted relative to the beginning of the input window, the number of steps in the output window.

  - Parameters of a neural network element with the Dense architecture: multipliers for calculating the number of neurons on layers, activations on layers.

  - Parameters of a neural network element with the RNN architecture: the number of GRU neurons on layers, the number of time-distributed neurons on the layers of the decoding block.

  - Parameters of a neural network element with CNN architecture: size of filters on layers, number of filters on layers, size of the maximum selection window, number of neurons on layers of the decoder.

    - Parameters of a neural network element with TCN architecture: regularization, filter size, extensions on layers, activation, number of encoders, type of layer before the output layer.

    - Parameters of the neural network element with the Transformer architecture: regularization in the encoder, the number of attention heads, the number of coding blocks, multipliers for calculating the number of neurons on the layers of encoder.

    - Training settings of a neural network element: training time interval, names and IDs of the training markups, maximum training duration, ratio between the training and the validation sample, maximum number of epochs for training, number of epochs during which there must be no validation losses when training is stopped early, chart resolution to display the training results, batch (dataset for training) size, number of blocks, inference mode, training mode, automatic data division into blocks, memory size used for training, information on whether to initialize the model weights with the values from the previous training results and/or shuffle the data.

    - Information about the training results of the neural network element: training queue (IDs and names of ML model elements that are waiting in the queue for training), training status, names and IDs of the training elements, the number of blocks into which the training dataset is divided, name of the user who started the training of the element, training duration, date and time of the training beginning and end, duration of the data time intervals in the training set, the number of UTG nodes included in the training set, training and validation errors, prediction of the trained ML model on the training set.

    - Settings for elements based on diagnostic rules: information on whether to interpret the impossibility to evaluate a condition as a rule execution, time filtering settings: interval type, years, days, days of the week, and the time interval during which to validate the input data in accordance with the specified rule; tag behavior condition settings: tag for which the condition is added, tag behavior, rule execution condition, number of UTG steps, tag threshold value, the minimum number of times a rule is triggered before logging an incident, value of the first level differential, time interval between the adjacent trend estimates, change threshold value, direction of the tag value change, tag value, maximum tag deviation from the specified value, the direction of change in tag value spread, indicator of whether the rule uses a pause and pause settings: minimum and maximum timeouts, group and logical operators used.

  A system administrator or a user with the **Manage ML models** rights set in the **Models** section can enter and/or upload the data.

- Information about markups: ID, name and description of the markup, interval used to calculate data on UTG, markup color, time filtering settings: interval type, years, days, days of the week, and the time interval during which to validate the input data in accordance with the specified markup conditions; tag behavior condition settings: tag for which the condition is added, tag behavior, rule execution condition, number of UTG steps, tag threshold value, the minimum number of times a rule is triggered before logging an incident, value of the first level differential, time interval between the adjacent trend estimates, change threshold value, direction of the tag value change, tag value, maximum tag deviation from the specified value, the direction of change in tag value spread, indicator of whether the rule uses a pause and pause settings: minimum and maximum timeouts, group and logical operators used.

  A system administrator or a user with the **Manage ML models** rights set in the **Models** section can enter and/or upload the data.

- Information security event logs: information security event ID, date and time of the information security event, type of information security event, subtype of information security event, severity level of the information security event, the name of the user whose actions resulted in registration of the information security event, the IP address of the computer from which the user performed the actions logged into the information security event log, the result of the information security event, a brief summary of the information security event, a detailed description of the information security event.

  The IP addresses of computers that established a connection to the web interface of the application are indicated in the information security event logs.

  The data is generated by Kaspersky MLAD automatically.

Kaspersky MLAD stores information security event logs for the time period specified in the **Storage time for information security event logs (days)** when configuring security settings. The program also deletes early entries in the information security event log when exceeding the space allocated for storing information security events set in **Volume of information security event logs (MB)**.

- Kaspersky MLAD container logs: event date and time, event severity level, name of the container for which the event is registered, event description.

  The data is generated by Kaspersky MLAD automatically.

  Kaspersky MLAD stores container logs for two days.

The logging system (Grafana) does not transmit users' data to Kaspersky or any third-party servers. You can read the procedure for storing and processing data in the logging system in the Grafana Logging System User Guide.

Data processed on users' computers

When working with the Kaspersky MLAD web interface, the following data is stored in the browser cookie files:

- Individual JSON Web Tokens to support a user session for connecting to the application web interface. An individualized token is stored in the user's browser cookie files for the user inactivity period defined when configuring the security settings.
- ID of the running Grafana session, if the user views the application logs. The Grafana session ID is stored in the user's browser cookie files for 30 days.

The user browser also stores data that is used to display the web interface: the last used localization language of the application web interface, the last used option for displaying the main menu (hidden or maximized display), the last used values of the time interval, preset, date and time, ML model branch, and the chart display settings in the **Monitoring**, **History**, and **Time slice** sections, the last used page numbering settings, the last set filters for displaying data in the **Event Processor** section, the last used values of the incident status and cause in the **Incidents** section, information about the "Tags for event presets #N" presets, generated for a registered incident, information about the current installed version of Kaspersky MLAD. This data is stored in the browser indefinitely. You can delete this data from the browser local storage yourself.

When exporting incidents, the application saves an XLSX file with the following data to the user computer:

- Name of monitored asset
- Period during which incidents were uploaded
- ID of the registered incidents
- Date and time when the incidents were registered
- Registered incidents statuses
- Names of the groups that include the registered incidents
- Names and IDs of the top tags having the greatest impact on the incidents registration
- Top tag values
- Top tags measurement units

- Top tags descriptions
- Name of the ML models that registered the incidents
- Name of the detectors that registered the incidents.

When exporting information security event logs from the Grafana logging system, the application saves a CSV file with the following data to the user computer:

- IDs of the information security events
- Date and time when the information security events occurred
- Information security events types
- Information security events subtypes
- Information security events severity levels
- Names of the users whose actions resulted in the registration of the information security events
- IP addresses of the computers from which the users performed the actions stored in the information security event log
- Information security event outcomes
- Brief summaries of the information security events
- Detailed descriptions of the information security events.

When exporting container logs from the Grafana logging system, the application saves a CSV file with the following data to the user computer:

- Date and time when the events occurred
- Event severity levels
- Name of the container for which the events are registered
- Event description.

When exporting asset and tag configuration, the application saves an XLSX file with the following data to the user computer:

- Asset type ID
- Unique name of the asset type
- Names of the special asset type settings (if any)
- Asset type description (if any)
- Asset ID
- Asset name

- Unique name of an asset within its parent asset
- Asset description (if any)
- Name of the parent asset to which the asset belongs (if any)
- Parent asset ID (if any)
- Names of the special asset settings (if any)
- Values of the special asset settings (if any)
- Tag ID
- Unique name of the tag
- Unique alternative name of the tag (if any)
- Tag description
- Name of the parent asset to which the tag belongs (if any)
- Parent asset ID
- Tag type (if any)
- Tag measurement units
- Lower and upper blocking thresholds (if any)
- Lower and upper signaling thresholds (if any)
- Lower and upper measurement confidence thresholds (if any)
- Lower and upper boundaries for displaying the tag values on charts (if any)
- The expression used to calculate the tag value from the value passed to Kaspersky MLAD
- Tag comment
- Location coordinates of the monitored asset sensor along the abscissa, ordinate, and applicate axes (if any).

When exporting presets, the application saves a JSON file with the following data to the user computer:

- Preset name
- Preset ID
- ID of the user who created the preset or uploaded it to the application
- IDs of the tags included in the preset
- Preset sequential number for sorting
- Preset icon.

- When using a preset to display data in the **Time slice** section, the application also saves the following data:
  - Text on the abscissa axis of the chart in the **Time slice** section
  - Name of the expression used to calculate the tag values
  - Text on the ordinate axis of the chart in the **Time slice** section
  - Expression used to calculate the tag values
  - Preset chart color in the **Time slice** section.

When exporting Kaspersky MLAD settings, the application saves configuration files with the following data to the user's computer:

- A file with the settings of the incident statuses, which contains the following data:
  - Incident status ID
  - Name of the incident status in Russian
  - Name of the incident status in English
  - Ordinal number of the incident status for sorting
  - Information on whether to display registered incidents with this status.
- A file with the settings of the incident causes, which contains the following data:
  - Incident cause ID
  - Name of the cause of the incident
  - Sequential number of the cause of the incident to be sorted.
- A file with the settings of the time intervals for displaying data on the **Monitoring**, **History**, and **Time slice** charts, which contains the following data:
  - Time interval ID
  - Name of the time interval in Russian
  - Name of the time interval in English
  - Ordinal number of the time interval for sorting
  - ID of the user who created the time interval
  - ID of the user who last changed the time interval
  - Time interval value in milliseconds.
- Settings of Kaspersky MLAD services and connectors:
  - Settings IDs

  - Names of the settings in the Kaspersky MLAD database
  - Types of the entered values
  - Entered or selected values
  - Name of the group to which the current setting belongs
  - Serial number of the setting displayed in the current section
  - Requirements for the setting value.
- The Stream Processor configuration file containing the following data:
  - IDs of tags processed by Stream Processor
  - Values of the tag processing settings.

    > The values of the tag processing settings are set by Kaspersky experts individually for each monitored asset.

- Configuration files of the MQTT Connector, AMQP Connector, and WebSocket Connector containing the following data:
  - Tag IDs obtained from the MQTT Connector, AMQP Connector, or WebSocket Connector
  - Tag timestamp measurement units
  - Type of the received data
  - Template format for decoding the received data type.
- The OPC UA Connector configuration file containing the following data:
  - Tag ID
  - Name of the asset to which the tag belongs
  - Data type passed to the tag value.
- The Event Processor configuration file containing the following data:
  - List of event parameters to be processed
  - Time and time scale for event processing
  - Order and relationship of the event parameters for display on the relationship graph in the **Event history** section.
- The communication data package for the KICS Connector containing the following data:
  - Public key of the Kaspersky Industrial CyberSecurity for Networks server certificate in the encrypted form, as well as the certificate issued by the Kaspersky Industrial CyberSecurity for Networks server for the KICS Connector (with the private key).

  The contents of the file are encrypted with the password that was set when the KICS Connector was added or when a new communication data package was created for this connector.

  - KICS Connector configuration data: the name of the Kaspersky MLAD user for connecting to the Kaspersky Industrial CyberSecurity for Networks server, the KICS Connector ID, and the address of the Kaspersky Industrial CyberSecurity for Networks server for connection.

Folders for storing application data

Kaspersky MLAD uses the following directories and subdirectories for storing data:

- Application directories (mlad-release-4.0.2-<installation build number> by default):
  - . – root directory of the application. It is used to store configuration files, Kaspersky MLAD installation and update logs, scripts for installing, updating, starting, and stopping Kaspersky MLAD, and the distribution package signatures. The root directory of the application contains notes on the current release of Kaspersky MLAD (Release Notes).
  - ./data – directory for storing data that is loaded using the HTTP Connector.
  - ./containers – directory for storing an archive of containers for Kaspersky MLAD services. Containers of Kaspersky MLAD services are installed to Docker from this archive.
  - ./legal – directory for storing the text of the End User License Agreement, the date of its acceptance by the user, and the legal_notices.txt file, which contains information about third-party code.
  - ./ssl – directory for storing the script for generating a self-signed certificate that provides an HTTPS connection to the Kaspersky MLAD user's browser.
  - ./ssl/tokens – directory for storing a JWT (JSON Web Token) key.
  - ./ssl/nginx – directory for storing certificates supporting an HTTPS connection with the browser of the Kaspersky MLAD user.
  - ./ssl/public_cert – directory for storing public keys used to verify the digital signature of the distribution package.
  - ./upgrade_backup-<version number>-<build number> – directory for storing the backup copies of Kaspersky MLAD that are created during an update of Kaspersky MLAD. The contents repeat the structure of the root directory where Kaspersky MLAD is installed.
  - ./backup-<version number>-<date and time of backup> – directory for storing backup copies of Kaspersky MLAD created during backup. The contents repeat the structure of the root directory where Kaspersky MLAD is installed.
  - ./volumes_backup_<date of deletion> – directory for storing backup copies of Docker **volumes** that are created during removal of Kaspersky MLAD.
- Directory /var/lib/docker/volumes/:
  - ./mlad-release-<version number>-<installation build number>_postgres-volume – directory for storing Postgres database files.

  - ./mlad-release-<version number>-<installation build number>_inflxdb-volume – directory for storing Time Series Database files.
  - ./mlad-release-<version number>-<installation build number>_logger-volume – directory for storing the logging subsystem files.
  - ./mlad-release-<version number>-<installation build number>_webstatic-volume – directory for storing static data of the application web interface.
- /etc/hosts – service file describing the mapping between IP addresses and host names of the external servers.

Application files can be modified by an administrator or by the user who unpacked the archive containing the installation script and all the files required for installation of Kaspersky MLAD.

> Deleting or modifying any file of Kaspersky MLAD can negatively impact the performance of the application.

System administrator tasks

This section contains a description of the system administrator tasks performed in the administrator menu of the application.

Managing user accounts

This section contains information about managing Kaspersky MLAD user accounts.

Kaspersky MLAD user accounts can be managed only by system administrators.

To ensure that users securely work with Kaspersky MLAD, install a trusted certificate for connecting to the web interface and create an account for each user.

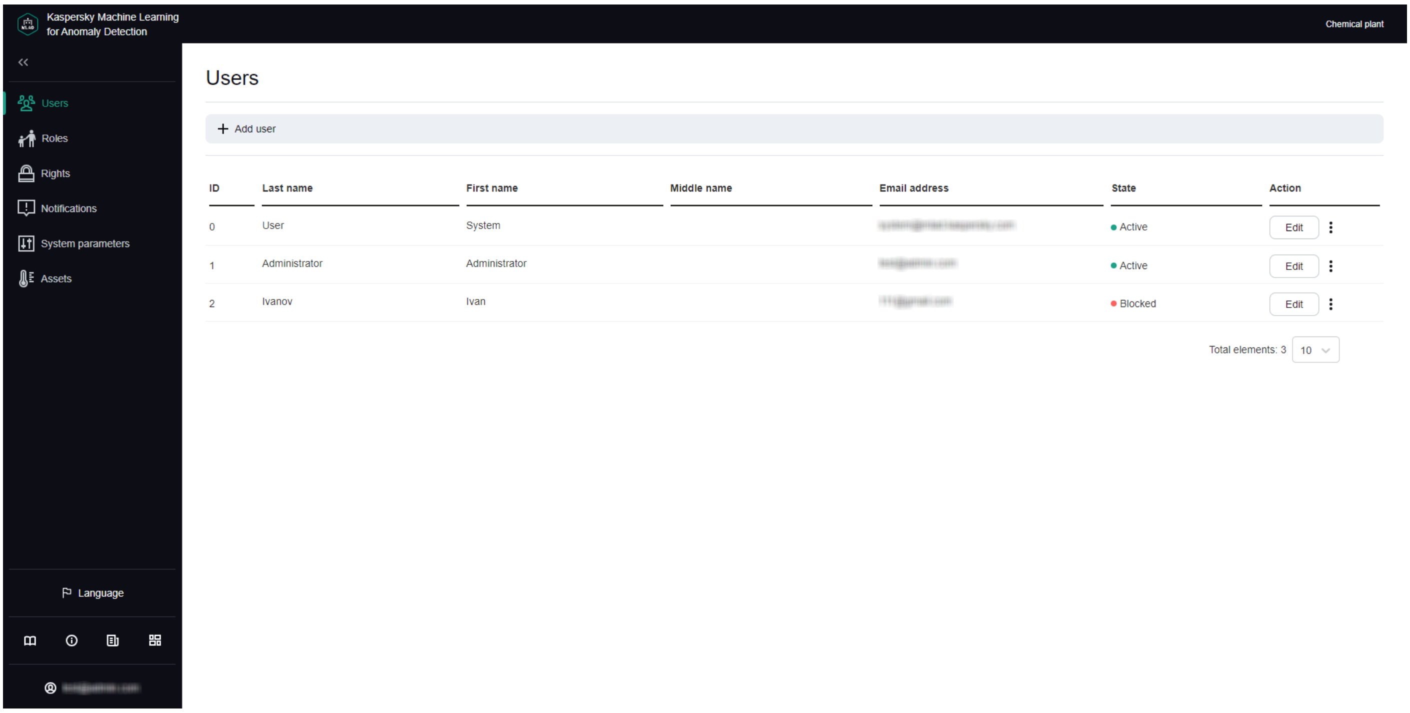
All created user accounts and **information about them** are displayed in the table tn the **Users** section of the administrator menu.

- **ID** is the user identifier.
- **Last name** refers to the last name of the user.
- **First name** refers to the first name of the user.
- **Middle name** refers to the middle name of the user.
- **Email address** refers to the user's email address.
- **State** is a parameter that describes the blocking status of a user account. If a user is blocked, a red dot with the **State** value appears in the **Blocked** column. If the user is unblocked, the **State** column shows a green dot with the value **Active**.
- **Action** is a button that lets you change the user account.

When installing the application, a special `User System` account is created. This account is not intended for use by personnel when working with Kaspersky MLAD. This account cannot be used to connect to the application web interface. To clarify whether or not you can change its settings, you are advised to consult with Kaspersky experts or a certified integrator.

If necessary, you can also add and edit user accounts. Kaspersky MLAD does not allow you to delete user accounts. To prevent a specific account from accessing Kaspersky MLAD web interface, it is recommended to block this account. You can unblock this user account later if necessary. If an account was locked when the number of unsuccessful login attempts for that user was reached, you can unblock this account before the blocking period expires. You can specify the number of unsuccessful authorization attempts and the account blocking period when configuring the security settings of Kaspersky MLAD.

Next to each account, there is a vertical menu ⋮ that lets you revoke authentication tokens or view the list of rights for the specific user account.



ID	Last name	First name	Middle name	Email address	State	Action
0	User	System		[redacted]	● Active	Edit
1	Administrator	Administrator		[redacted]	● Active	Edit
2	Ivanov	Ivan		[redacted]	● Blocked	Edit

Total elements: 3 10

Users section

Creating a user account

Kaspersky MLAD user accounts can be managed only by system administrators.

To create a user account:

1. In the lower-left corner of the page, click the button.

   You will be taken to the administrator menu.

2. Select the **Users** section.

3. Click the **Add user** button.

   The **Add user** window opens.

4. In the **Last name** field, enter the last name of the user.

5. In the **First name** field, enter the first name of the user.

6. If necessary, enter the middle name of the user in the **Middle name** field.

7. In the **Email address** field, enter the email address of the user.

8. In the **Password** field, enter a password for the user account.

   The password must meet the following requirements:

   - Must contain the minimum number of characters defined in the **Minimum password length** setting.
   - Must contain letters of the English alphabet, numerals and/or special characters in accordance with the password policy that was set when configuring the security settings.

9. In the **Confirm password** field, type the password again to confirm the password for the user account.

10. Click the **Save** button.

    Information about the new user will be displayed in the table. If necessary, you can modify user accounts and revoke their authentication tokens

When creating an account, you cannot assign a role to a user. You can assign a role to a user only when editing the user account.

Editing a user account

Kaspersky MLAD user accounts can be managed only by system administrators.

When you edit a user account, you can assign the desired role to the user. You can also block or unblock a user account. If an account is blocked, the user cannot log in to Kaspersky MLAD.

If the user was logged in when the account was blocked, the application session is active until one of the following conditions is met:

- The user logged out of the account.
- The application automatically terminated the connection session when the authentication token for the user account expired.
- Authentication tokens have been revoked for the user account.

To edit a user account:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Users** section.

3. Click the **Edit** button in the row of the user account that you want to edit.

   The **Edit user** window opens.

4. If necessary, do the following:

   a. In the **Last name** field, enter a new last name for the user.

   b. In the **First name** field, enter a new first name for the user.

   c. In the **Middle name** field, enter a new middle name for the user.

5. In the **Roles** field, assign a role for the user account by selecting the corresponding check box.

6. If you need to change the password, enter the new password in the **Password** and **Confirm password** fields.

   The new password must meet the following requirements:

   - Must not match previously used passwords. The specific number of most recently used passwords that must not be reused is defined by the value of the **Number of user passwords stored in history** setting.

- Must contain the minimum number of characters defined in the **Minimum password length** setting.
- Must contain letters of the English alphabet, numerals and/or special characters in accordance with the password policy that was set when configuring the security settings.

7. If you want to block or unblock a user account, perform one of the following actions:

   - If you want to unblock a user account, set the **State** toggle switch to the **Active** position.
   - If you want to block a user account, set the **State** toggle switch to the **Blocked** position.

   Kaspersky MLAD does not allow you to delete user accounts. If you want to prevent a specific user account from accessing Kaspersky MLAD, it is recommended to block this user account.

8. Click the **Save** button.

   The updated information about the user will be displayed in the table. If the password for a user account is changed, Kaspersky MLAD automatically terminates the user session of the user account whose password was changed.

Revoking authentication tokens for a user account

> Kaspersky MLAD user accounts can be managed only by system administrators.

After a user connects to the Kaspersky MLAD web interface, an individualized token is created so that the user authorization in the application can be saved between connection sessions to the application web interface, including when the browser is restarted. If a user is authorized on multiple assets, a token is created for each user session. If necessary, you can revoke tokens for a user account at any time. For the user whose tokens are revoked, their work session in the application is terminated simultaneously on all assets where they were authorized. Revoking tokens may be useful if you need to immediately terminate application connection sessions for a specific user.

To revoke a token or tokens for a user account:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Users** section.

3. Click the vertical menu ⋮, which is located in the row of the user account whose authentication tokens you want to revoke.

4. Select **Revoke tokens**.

5. In the confirmation window, click **Yes**.

   The user account tokens are revoked, and the user session is terminated.

Viewing access rights for a user account

Kaspersky MLAD user accounts can be managed only by system administrators.

In the **Users** section, you can view the list of rights for a specific user account.

To view the access rights for a user account:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Users** section.

3. Click the vertical menu ⋮, which is located in the row of the user account whose list of access rights you want to view.

4. Select **List of rights**.

The page displays a window containing information about the role and access rights of the selected user account.

Manage roles

In Kaspersky MLAD, you can use common roles to restrict user access to application functions depending on the tasks performed by specific users.

A *role* is a set of rights to access application functions that you can assign to a user.

Accounts with the following roles can be used to access application functions:

- The system administrator role is created automatically during installation of the application. The system administrator role is automatically assigned to the first user created during installation of Kaspersky MLAD. A user with the system administrator role has access to all functions of the application. The system administrator role cannot be modified or removed.

- A user role is created manually in the **Roles** section. Access to application functions depends on the list of rights granted to the user role. The number of user roles is unlimited.

The **Roles** section displays a table with **information about all created roles**.

- **ID** is the digital ID of the user role.
- **Role** is the name of the user role.
- **State** indicates whether this role is in use.
- **Rights** is a button that lets you view a list of the rights of a user role in Kaspersky MLAD.
- **Created** refers to the date and time when the user role was created.
- **Updated** refers to the date and time when the user role was updated.

Role management is available to system administrators.

Creating role

Role management is available to system administrators.

You can create user roles and select the access rights to application functions for them. After an active role is created, it will become available for assignment to application users.

To create a role:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Roles** section.

3. Click the **Create** button.

   The **Creating role** pane will appear on the right.

4. In the **Role name** field, specify the required role name.

   You can enter up to 30 characters.

5. If necessary, enter a new description for the tag in the **Role description** field.

6. To grant access rights to a role, do the following:

   a. Click the **Select rights** button.

      The **Grant rights to role** pane appears on the right.

   b. In the list of rights, select the access rights to application functions that you want to grant to the role.

      When you select **Rights to all actions**, all system administrator functions will be available to the role.

   c. Click the **Save** button.

7. To enable the use of the role for application users, set the **State** switch to the **Active** position.

8. Click the **Save** button.

Editing role

Role management is available to system administrators.

To change a role:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Roles** section.

3. Click the **Edit** button.

   The **Editing role** panel appears on the right.

4. In the **Role name** field, specify a new role name.

   You can enter up to 30 characters.

5. If necessary, enter a new description for the role in the **Role description** field.

6. To edit the access rights of a role, do the following:

   a. Click the **Number of rights** button.

      The **Grant rights to role** pane appears on the right.

   b. In the list of rights, change the selection of access rights to application functions that you want to grant to the role.

      When you select **Rights to all actions**, all system administrator functions will be available to the role.

   c. Click the **Save** button.

7. Perform one of the following actions:

   - If you need to use a role for application users, set the **State** switch to the **Active** position.

   - If you need to disable the use of a role for application users, set the **State** toggle switch to the **Inactive** position.

8. Click the **Save** button.

Deleting role

> Role management is available to system administrators.

You can delete user roles that are not assigned to Kaspersky MLAD users.

System administrator role cannot be deleted.

To delete a role:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Roles** section.

3. Select the check boxes next to the names of the roles that you want to remove.

4. Click the **Delete** button.

5. In the opened window, click **Yes** to confirm deletion.

Viewing access rights for a role

Role management is available to system administrators.

In the **Roles** section, you can view a list of access rights to application functions for users with a specific role.

To view the access rights for a role:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Roles** section.

3. Click the **List of rights** button in the line of the role for which you want to view the list of rights.

   A window opens on the page with information about access rights to application functions for the selected role.

Managing incident notifications

This section describes how to manage notifications for incident registration. Notifications are emailed to the users for whom these notifications have been configured.

Only system administrators can manage incident notifications.

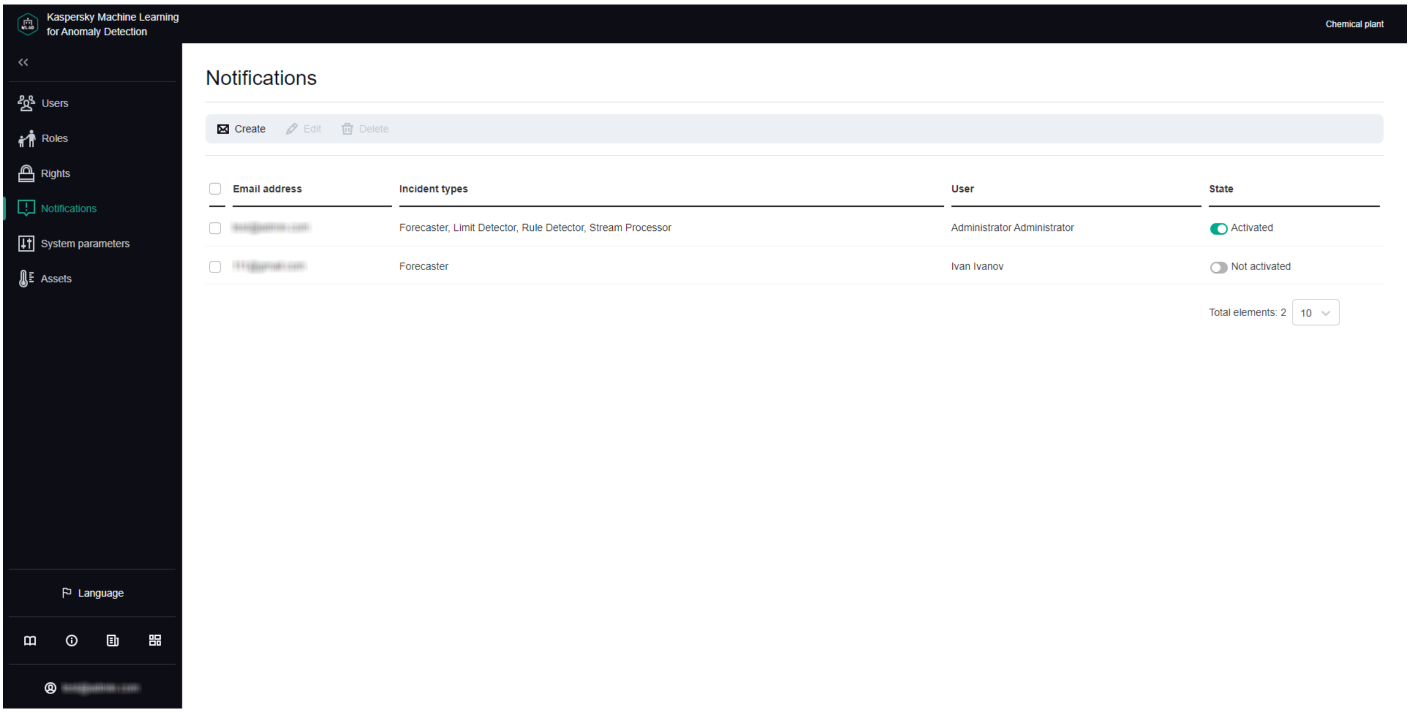
The Mail Notifier service must be configured and started in advance.

All created notifications about incidents and **information about them** are displayed in the **Notifications** section in the administrator menu.

- **Email address** is the user email address to which the incident notifications are sent.
- **Incident types** – the type of incidents that the user receives notifications about. You can receive incident notifications registered by the Forecaster, Limit Detector, Rule Detector, and the Stream Processor service.
- **User** – the last name and first name of the user who receives incident notifications.
- **State** lets you enable or disable sending of incident notifications.

If necessary, you can change the number of notifications displayed on one page.

You can create, edit, and delete notifications regarding specific incidents for Kaspersky MLAD users.



Notifications

Email address	Incident types	User	State
[redacted]	Forecaster, Limit Detector, Rule Detector, Stream Processor	Administrator Administrator	Activated
[redacted]	Forecaster	Ivan Ivanov	Not activated

Total elements: 2 10

Notifications section

Creating an incident notification

Only system administrators can manage incident notifications.

To create an incident notification for a user:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Notifications** section.

3. On the opened page, click the **Create** button.

   The **Create notification** window opens.

4. In the **User** drop-down list, select the user for whom you want to create a notification.

   The **User** list displays the last names and first names of users specified when user accounts were created.

5. In the **Email address** field, specify the email address to which incident notifications are sent.

   By default, Kaspersky MLAD automatically fills in the **Email address** field with the address specified for the selected user when the user account was created.

6. Specify the types of incidents for which the application will send notifications:

   - If you want to configure a notification about predicted tag values, select the **Forecaster** check box.

- If you want to configure a notification about a tag value approaching the blocking threshold, select the **Limit Detector** check box.
- If you want to configure a notification about a tag reaching the threshold set for a diagnostic rule, select the **Rule Detector** check box.
- If you want to configure a notification about the termination or interruption of the input data stream for a specific tag, or about the detection of observations that arrived too soon or too late, select the **Stream Processor** check box.

7. In the **Delivery language** field, select the language of the delivered incident notifications.

   By default, the current localization language of the Kaspersky MLAD web interface is used for incident notifications. It is available in English and Russian.

8. To enable sending of notifications, set the **State** toggle switch to the **Activated** position.

9. Click the **Save** button.

Information about the new notification will be displayed in the table. If necessary, you can edit or delete notifications.

Editing an incident notification

> Only system administrators can manage incident notifications.

To edit an incident notification:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Notifications** section.

3. Select the check box next to the notification that you want to change and click the **Edit** button.

   > The **Edit** button is available if only one notification is selected.

4. Make the necessary changes.

5. If necessary, enable or disable sending incident notifications using the **State** toggle switch.

6. Click the **Save** button to save the changes.

The updated information about the notification will be displayed in the table. If necessary, you can delete notifications.

Enabling and disabling sending notifications about incidents

> Only system administrators can manage incident notifications.

Kaspersky MLAD allows you to temporarily disable sending of notifications instead of deleting their configuration. Information about notifications is saved in the **Notifications** section. You can enable sending of a notification at any time.

To enable or disable sending of incident notifications:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Notifications** section.

3. Perform one of the following actions:

   - If you want to enable sending incident notifications, set the toggle switch in the **State** column to the **Activated** position for the relevant notification.

   - If you want to disable sending incident notifications, set the toggle switch in the **State** column to the **Not activated** position for the relevant notification.

Deleting an incident notification

> Only system administrators can manage incident notifications.

To delete an incident notification:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Notifications** section.

3. Select the check box next to the notification that you want to delete and click the **Delete** button.

   The **Delete** button is available if at least one notification is selected. You can select multiple notifications at the same time.

4. In the opened window, click **Yes** to confirm deletion.

Information about the notification will be deleted from the table.

Kaspersky MLAD lets you temporarily disable sending of notifications instead of deleting them.

Configuring Kaspersky MLAD

This section contains instructions on configuring the settings of Kaspersky MLAD services and connectors, as well as on configuring security settings, logging levels for application services, settings for displaying the application menu, and on managing typical statuses and causes of incidents.

Configuring the main settings of Kaspersky MLAD

Kaspersky MLAD lets you specify the name of the monitored asset, web address and IP address for connecting users to the application web interface, and the frequency of receiving new data from the monitored asset. The name of the monitored asset will be displayed in each section of the Kaspersky MLAD web interface.

> System administrators can configure the main settings of Kaspersky MLAD.

To configure the main settings of Kaspersky MLAD:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **System parameters** → **Main** section.

   A list of options appears on the right.

3. In the **Name of monitored asset** field, specify the name of the monitored asset.

4. In the **Application web address** field, specify the web address of the application.

5. In the **Application connection IP address** field, specify the IP address of the application.

6. In the **Interval for receiving data from the Message Broker service (ms)** field, specify the interval for updating telemetry data in the application web interface.

   The higher the specified parameter value, the less frequently the data is updated.

7. In the **Interval for receiving incident statistics from the database (ms)** field, indicate how frequently data on incidents registered by the application should be updated in the application web interface.

8. In the **Monitored asset time zone** drop-down list, select the required time zone.

9. Click the **Save** button.

Configuring the security settings of Kaspersky MLAD

Kaspersky MLAD lets you specify the conditions for blocking user accounts, the user inactivity period in accordance with the enterprise security policy, and the settings for storing information security event logs in the Kaspersky MLAD database. Information security event logs are automatically written to the database. If necessary, you can specify the settings of an external system to which the information security event logs should be sent.

> System administrators may be responsible for configuring the security settings of Kaspersky MLAD.

To configure the main settings of Kaspersky MLAD:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **System parameters** → **Security** section.

   A list of options appears on the right.

3. In the **Authorization parameters** block, do the following:

   a. In the **Number of authentication attempts** field, specify the number of unsuccessful authorization attempts. When this number is reached, Kaspersky MLAD blocks the corresponding user account.

   b. In the **User lock duration (sec)** field, specify the time period (in seconds) to block a user account after reaching the specified number of unsuccessful authorization attempts.

   c. In the **User inactivity period (min)** field, specify the permissible duration of an inactive user session (in minutes).

      When the specified time period is reached, Kaspersky MLAD automatically terminates the inactive user session.

   d. If you need to prevent users from ignoring the password change recommendation when they connect to the application web interface for the first time, turn on the **Require password change on first login** toggle switch.

4. In the **Password policy** settings block, do the following:

   a. In the **Number of user passwords stored in history** field, specify the number of most recent user passwords that are stored in the application.

      You can specify a value starting with `1`.

      When the user password is changed, the new password must not match any passwords stored in Kaspersky MLAD. The application stores passwords in encrypted form.

   b. In the **Password expiration period (days)** field, specify the number of days during which the user can use their current password to connect to the application without changing it.

   c. In the **Minimum password length** field, specify the minimum number of characters for user passwords.

      You can specify a value in the range of `8 to 128`.

   d. If your security policy stipulates that user passwords must contain uppercase letters of the English alphabet, turn on the **Require use of uppercase letters of the English alphabet (A-Z)** toggle switch.

   e. If your security policy stipulates that user passwords must contain lowercase letters of the English alphabet, turn on the **Require use of lowercase letters of the English alphabet (a-z)** toggle switch.

   f. If your security policy stipulates that user passwords must contain numerals, turn on the **Require use of numerals (0-9)** toggle switch.

   g. If your security policy stipulates that user passwords must contain special characters, turn on the **Require use of special characters (_!@#$%^&*)** toggle switch.

5. In the **Storage parameters for information security event logs** block, do the following:

   a. In the **Volume of information security event logs (MB)** field, specify the volume limit (in megabytes) for storing information security event logs in the database.

      If the field is blank, Kaspersky MLAD stores all information security event logs for the time period specified in the **Storage time for information security event logs (days)** setting.

      If the specified volume of information security event logs in the database is exceeded, Kaspersky MLAD deletes the oldest entries.

b. In the **Storage time for information security event logs (days)** field, specify the number of days to store information security event logs in the database.

6. Click the **Save** button.

Configuring the Anomaly Detector service

In Kaspersky MLAD, an ML model can contain the following detectors:

- Limit Detector detects anomalies whenever the tag value falls below the minimum value or exceeds the maximum value.
- Forecaster predicts the current behavior of an object based on data about its behavior in the recent past.
- XGBoost with a certain probability detects anomalies in the monitored asset data based on the data sample for the examined time interval learned by the XGBoost classifier.
- Rule Detector builds predictions for the tag values during normal operation of the monitored asset and registers incidents whenever one or multiple rules are triggered.

You can configure the procedure for detecting anomalies based on the specific features of your monitored asset by enabling or disabling the necessary detectors in the Anomaly Detector service settings.

> System administrators can configure the Anomaly Detector service.

To configure the settings of the Anomaly Detector service in Kaspersky MLAD:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **Anomaly Detector**.

   A list of options appears on the right.

3. Enable or disable the Limit Detector using the **Use Limit Detector** toggle switch.

4. Enable or disable the Forecaster detector using the **Use Forecaster detector** toggle switch.

5. Enable or disable the XGBoost detector using the **Use XGBoost detector** toggle switch.

6. Enable or disable use of the Rule Detector using the **Use Rule Detector** toggle switch.

7. Enable or disable the function for skipping gaps in the incoming data stream using the **Skip gaps in data** toggle switch.

8. In the **Maximum number of records requested from the Message Broker service** field, enter the number of records that must be requested from the Message Broker service for subsequent processing in the Anomaly Detector.

9. In the **Number of messages sent in one block to the Message Broker service** field, enter the number of incidents that must be sent to the Message Broker service at one time.

10. In the **Number of simultaneously running models** field, enter the maximum number of ML models that can analyze telemetry data at the same time.

    > For maximum performance of Kaspersky MLAD, the number of ML models running at the same time must not exceed 80% of the number of cores of the server where Kaspersky MLAD is installed.

11. Click the **Save** button.

Configuring the Keeper service

Kaspersky MLAD uses the Keeper service to route telemetry data that should be saved in the database. You can configure the settings that define the rate of incoming data received from connectors and external sources, and the volume of data that is saved in the Kaspersky MLAD database.

> System administrators can configure the data routing settings in Kaspersky MLAD.

To configure the Kaspersky MLAD data routing settings:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **System parameters** → **Keeper** section.

   A list of options appears on the right.

3. Perform one of the following actions:

   - To save both known and unknown tags from external sources to the database, turn on the **Save all tags** toggle.

   - To save only the tags that are known to the application, turn off the **Save all tags** toggle.

4. In the **Timeout for receiving tags (ms)** field, enter the maximum timeout (in milliseconds) for receiving the values of tags.

5. In the **Timeout for receiving incidents (ms)** field, enter the maximum timeout (in milliseconds) for receiving incidents.

6. In the **Timeout for receiving metrics (ms)** field, enter the maximum timeout (in milliseconds) for receiving metrics.

7. Click the **Save** button.

Configuring the Mail Notifier service

Kaspersky MLAD uses the Mail Notifier service to notify users when incidents are registered by the application.

System administrators can configure the Mail Notifier service.

Configuring the Mail Notifier service is optional; it is performed if an SMTP server is configured in the monitored asset network.

To configure the Mail Notifier service:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **Mail Notifier**.

   A list of options appears on the right.

3. In the **SMTP server address** field, enter the IP address of the SMTP server.

4. In the **SMTP server port** field, enter the port of the SMTP server.

5. In the **SMTP server user name** field, enter the user name for the SMTP server.

6. In the **SMTP server password** field, enter the password for the SMTP server.

7. If necessary, enable secure TLS connection using the **Use TLS connection** toggle switch.

   By default, use of a secure TLS connection is disabled.

   To avoid compromising the received and/or sent data, it is recommended to enable the use of a secure TLS connection. It is recommended to use a secure TLS connection via the TLS-1.2 or TLS-1.3 protocol using a cipher suite from the list of recommended ciphers.

8. If you are using a secure TLS connection, do the following:

   - Upload the SMTP server certificate using the **Browse** button under **SMTP server certificate**.
   - Upload the key to the SMTP server certificate file using the **Browse** button under the **Key to SMTP server certificate** setting.

   It is recommended to use a certificate created according to the X.509 standard with a certificate key length of at least 4096 bits.

   To delete the certificate file or certificate key, click the **Clear** icon (🗑) in the corresponding field. To save the certificate file or certificate key on your computer, click the **Download** icon (⤓) in the corresponding field.

9. Click the **Save** button.

Configuring the Similar Anomaly service

Kaspersky MLAD uses the Similar Anomaly service to identify similar incidents and combine them into groups. In groups, you can view similar incidents that were registered at different times.

> System administrators can configure the Similar Anomaly service.

To configure the Similar Anomaly service:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **Similar Anomaly**.

   A list of service settings appears on the right.

3. In the **Minimum number of incidents in group** field, enter the minimum number of similar incidents for forming a group.

4. In the **Maximum number of incidents in group** field, enter the maximum number of incidents that can be put into one group.

   The larger the specified value, the more incidents the application can assign to one group.

5. In the **Maximum distance between similar incidents** field, enter the maximum distance that similar incidents can lag behind each other.

   You can specify a value in the range of `0` to `1`.

6. Click the **Save** button.

Configuring the Stream Processor service

The Stream Processor service gathers real-time telemetry data (input stream) received from the monitored asset at arbitrary points in time and converts this data to a UTG (output stream). Based on the accumulated data, the Stream Processor service determines the values of tags in the output data stream. After converting data into an output stream, the Stream Processor service forwards this data to the ML model for processing.

When converting incoming telemetry data, the Stream Processor service accounts for potential data losses (for example, if the network of the monitored asset temporarily goes down) and processes observations that were received in Kaspersky MLAD too early or too late. In these cases, the Stream Processor service generates default incidents and/or forwards default tag values to the output data stream.

The Stream Processor service can also compute derivative tags based on incoming telemetry data (for example, to calculate the moving average or average value of a group of tags).

> The Stream Processor service configuration file for uploading is provided by Kaspersky specialists or a certified integrator.

> System administrators can configure the Stream Processor service.

To configure the Stream Processor service:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **Stream Processor**.

3. In the **Fixed-interval sequence frequency (sec)** field, specify the period (in seconds) for which the Stream Processor service will process incoming telemetry data.

4. Using the **Browse** button under the **Configuration file** setting, add a file that contains configuration settings for the Stream Processor service.

   To delete the configuration file for the Stream Processor service, click **Clear** (🗑). To save the configuration file on your computer, click the **Download** icon (⤓).

5. Click the **Save** button.

Configuring the HTTP Connector

Kaspersky MLAD uses the HTTP Connector to receive data from CSV files during scheduled uploads of data using the `POST` method. You can download data via HTTP or HTTPS by specifying the relevant protocol in a request.

System administrators can configure the HTTP Connector.

The HTTP Connector does not support a secure connection. If you want to use a secure connection to receive and send data, it is recommended to use additional means to secure the network connection (for example, use a VPN) or use another method to prevent unauthorized access to the communication channel.

To configure the HTTP Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **HTTP Connector**.

   A list of options appears on the right.

3. Use the **Write data to the Message Broker service** toggle switch to enable writing data to the Message Broker service.

4. If necessary, use the **Save received file** toggle switch to enable the function for saving received CSV files.

5. In the **Size of written block (tag count)** field, specify the number of tags that are written to the Message Broker service at one time.

6. In the **Maximum size of uploaded file (MB)** field, specify the maximum size (in megabytes) of a file transmitted to the HTTP Connector.

   If you try to download a larger CSV file, the file would not be passed to the HTTP Connector.

7. Click the **Save** button.

Kaspersky MLAD will receive data from CSV files using the HTTP Connector.

The following is an example of sending a CSV file to the HTTP Connector via cURL over HTTP using the `POST` method to port 4999 of the Kaspersky MLAD server:

```
curl -F "file=@<file name>.csv" -X POST "http://<Kaspersky MLAD server IP address or
domain name>:4999/"
```

The HTTP Connector accepts CSV files with the following fields:

`timestamp;tag_name;value`

where:

- `timestamp` is the time stamp in the format %Y-%m-%dT%H:%M:%S.
- `tag_name` is the name of the tag.
- `value` is the tag value.

  If a tag value contains a fractional portion, use a dot to separate the integer from the fractional portion.

Configuring the MQTT Connector

Kaspersky MLAD uses the MQTT Connector to receive data and send messages about incident registration via the MQTT (Message Queuing Telemetry Transport) protocol.

> System administrators can configure the MQTT Connector.

To configure the MQTT Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **MQTT Connector**.

   A list of options appears on the right.

3. If necessary, use the **Use TLS connection** toggle switch to enable secure TLS connection.

   By default, use of a secure TLS connection is disabled.

   > To avoid compromising the received and/or sent data, it is recommended to enable the use of a secure TLS connection. It is recommended to use a secure TLS connection via the TLS-1.2 or TLS-1.3 protocol using a cipher suite from the list of recommended ciphers.

4. In the **MQTT broker (address:port)** field, specify the host name and port of the external MQTT broker that the MQTT Connector will interact with.

   The default value of this parameter is `mqtt_broker:1883`.

5. In the **User name for MQTT connection** field, enter the user name.

6. In the **Password for MQTT connection** field, enter the user's password.

7. If you enabled the use of a secure TLS connection and a self-signed certificate is installed on the MQTT broker, add the root certificate for the MQTT broker using the **Browse** button under the **CA certificate** setting.

To delete the certificate file, click the **Clear** icon (🗑). To save the certificate file on your computer, click the **Download** icon (⤓).

8. If you enabled the use of a secure TLS connection and client authentication is enabled on the MQTT broker, do the following:

   - Add the MQTT client application certificate by using the **Browse** button under the **Client certificate** setting.

   - Add the key to the MQTT client application certificate by using the **Browse** button under the **Key to client certificate** setting.

   > It is recommended to use a certificate created according to the X.509 standard with a certificate key length of at least 4096 bits.

   To delete the certificate file or certificate key, click the **Clear** icon (🗑) in the corresponding field. To save the certificate file or certificate key on your computer, click the **Download** icon (⤓) in the corresponding field.

9. In the **List of MQTT subscriptions for receiving tags** field, enter the name of the list of MQTT subscriptions from which the MQTT Connector will receive tag values.

   The default value of this parameter is `tags`.

10. In the **MQTT topic for publishing messages** field, specify the name of the topic where the MQTT Connector will publish messages about incident registration.

    If no value is defined for this setting, messages are not sent.

    This setting has no value by default.

11. In the **Data format** drop-down list, select the format to receive data from external systems and send incident alerts.

    The following options are available: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

    The default value of this parameter is `JSONBatch`.

    > If none of the incident data and alert formats suits you, you can contact Kaspersky Lab experts to add the required format.

12. If you have selected the `Topic` data format, add a configuration file containing the connector settings for this data format using the **Browse** button under the **Connector configuration file** setting.

    To delete the certificate file, click the **Clear** icon (🗑). To save the certificate file on your computer, click the **Download** icon (⤓).

13. If you need to recalculate the tag values based on the parameter values specified in the preset file, turn on the **Scale obtained tag values** toggle switch.

    By default, scaling of the received data is disabled.

14. Click the **Save** button.

Kaspersky MLAD will receive data and send messages about incident registration via the MQTT protocol.

Configuring the AMQP Connector

Kaspersky MLAD uses the AMQP Connector to receive data and send messages about incident registration via AMQP (Advanced Message Queuing Protocol).

> System administrators can configure the AMQP Connector.

To configure the AMQP Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **AMQP Connector**.

   A list of options appears on the right.

3. If necessary, use the **Use TLS connection** toggle switch to enable secure TLS connection.

   By default, use of a secure TLS connection is disabled.

   > To avoid compromising the received and/or sent data, it is recommended to enable the use of a secure TLS connection. It is recommended to use a secure TLS connection via the TLS-1.2 or TLS-1.3 protocol using a cipher suite from the list of recommended ciphers.

4. In the **AMQP broker (address:port)** field, specify the host name and port of the external AMQP broker that the AMQP Connector will interact with.

   The default value of this parameter is `rabbitmq:5672`.

5. In the **User name for AMQP connection** field, enter the user name.

6. In the **Password for AMQP connection** field, enter the user's password.

7. If you enabled the use of a secure TLS connection and a self-signed certificate is installed on the AMQP broker, add the root certificate for the AMQP broker using the **Browse** button under the **CA certificate** setting.

   To delete the certificate file, click the **Clear** icon (🗑). To save the certificate file on your computer, click the **Download** icon (⤓).

8. If you enabled the use of a secure TLS connection and client authentication is enabled on the AMQP broker, do the following:

   - Add the AMQP client application certificate by using the **Browse** button under the **Client certificate** setting.

   - Add the key to the AMQP client application certificate by using the **Browse** button under the **Key to client certificate** setting.

   > It is recommended to use a certificate created according to the X.509 standard with a certificate key length of at least 4096 bits.

   To delete the certificate file or certificate key, click the **Clear** icon (🗑) in the corresponding field. To save the certificate file or certificate key on your computer, click the **Download** icon (⤓) in the corresponding field.

9. In the **AMQP virtual host** field, specify the virtual host for establishing a connection between the AMQP Connector and the external AMQP broker.

The default value of this parameter is `/`.

10. In the **AMQP exchange point name for receiving tags** field, specify the name of the exchange point to receive tags from an external AMQP broker.

    If a value is not defined for this parameter, tags will not be received via the AMQP Connector.

    This setting has no value by default.

11. In the **List of AMQP subscriptions for receiving tags** field, specify the name of the list of subscriptions from which the AMQP Connector will receive tag values.

    The default value of this parameter is `#`.

12. In the **AMQP queue for receiving tags** field, specify the name of the queue for the AMQP connector. This field is optional.

13. In the **AMQP exchange point name for publishing messages** field, specify the name of the exchange point for sending messages about events.

    If no value is defined for this parameter, messages will not be sent. You can specify the same name that you indicated in step 10 of these instructions.

    This setting has no value by default.

14. In the **AMQP topic for publishing messages** field, specify the name of the topic where the AMQP Connector will publish messages about incident registration.

    The default value of this parameter is `alert`.

15. In the **Data format** drop-down list, select the format to receive data from external systems and send incident alerts.

    The following options are available: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

    The default value of this parameter is `JSONBatch`.

    > If none of the incident data and alert formats suits you, you can contact Kaspersky Lab experts to add the required format.

16. If you have selected the `Topic` data format, add a configuration file containing the connector settings for this data format using the **Browse** button under the **Connector configuration file** setting.

    To delete the connector configuration file, click the **Clear** icon (🗑). To save the connector configuration file on your computer, click the **Download** icon (⤓).

17. If you need to recalculate the tag values based on the parameter values specified in the preset file, turn on the **Scale obtained tag values** toggle switch.

    By default, scaling of the received data is disabled.

18. Click the **Save** button.

Kaspersky MLAD will receive data and send messages about incident registration via the AMQP protocol.

Configuring the OPC UA Connector

Kaspersky MLAD uses the OPC UA Connector to receive data over a protocol described by the OPC Unified Architecture specification.

System administrators can configure the OPC UA Connector.

The OPC UA Connector does not support a secure connection. If you want to use a secure connection to receive and send data, it is recommended to use additional means to secure the network connection (for example, use a VPN) or use another method to prevent unauthorized access to the communication channel.

To configure the OPC UA Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **OPC UA Connector**.

   A list of options appears on the right.

3. In the **Connection point** field, specify the connection address.

   For example: `opc.tcp://10.0.0.0:8001/freeopcua/server/`.

4. In the **OPC UA server connection timeout (sec)** field, specify the time period (in seconds) that the OPC UA Connector will attempt to establish a connection with the OPC UA server.

5. Using the **Browse** button under the **Configuration file** setting, add a file containing settings for configuring the OPC UA Connector.

   To delete the connector configuration file, click the **Clear** icon (🗑). To save the connector configuration file on your computer, click the **Download** icon (⤓).

6. In the **Historical data interval (sec)** field, specify the time interval (in seconds) for which the OPC UA Connector requests historical data stored on the OPC UA server.

   Enter `0` if you do not need to download historical data. Enter `-1` if you need to download all historical data.

7. In the **Start of historical data period (YYYY/MM/DD HH:MM:SS)** field, specify the start date and time of the period for which you want to download data from the OPC UA server.

8. In the **End of historical data period (YYYY/MM/DD HH:MM:SS)** field, specify the end date and time of the period for which you want to download data from the OPC UA server.

9. In the **Size of historical data block sent by OPC UA server (numvalues parameter)** field, specify the number of tags that will be transmitted in the historical data block sent to the OPC UA Connector from the OPC UA server.

10. In the **Size of historical data block sent to Message Broker service** field, specify the number of tags that will be transmitted in the historical data block sent from the OPC UA Connector to the Message Broker service.

11. Click the **Save** button.

Configuring the KICS Connector

Kaspersky MLAD uses the KICS Connector to receive data from Kaspersky Industrial CyberSecurity for Networks 4.0 and later and to send back incident registration messages.

The connector for integration with Kaspersky MLAD must be created and added to Kaspersky Industrial CyberSecurity for Networks in advance. For detailed information about creating and adding a connector, please refer to the *Adding a connector* section of *Kaspersky Industrial CyberSecurity for Networks Help Guide*.

> System administrators can perform integration with Kaspersky Industrial CyberSecurity for Networks version 4.0 or higher.

To configure the KICS Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **KICS Connector**.

   A list of options appears on the right.

3. Using the **Browse** button under the setting **Communication data package for KICS Connector (zip)** field, add the file containing the settings for configuring interaction between Kaspersky MLAD and Kaspersky Industrial CyberSecurity for Networks.

   For detailed information about creating a communication data package, please refer to the *Kaspersky Industrial CyberSecurity for Networks Help Guide*. The created communication data package must be saved on the computer where Kaspersky MLAD is installed.

   To delete a communication data package, in the **Communication data package for KICS Connector (zip)** field, click the **Clear** (🗑) icon. To save the communication data package on your computer, click the **Download** icon (⤓).

4. In the **Password for KICS Connector** field, enter the password that you specified when adding the connector to Kaspersky Industrial CyberSecurity for Networks.

5. If you need to send incident registration notifications to Kaspersky Industrial CyberSecurity for Networks, turn on the **Send messages to Kaspersky Industrial CyberSecurity for Networks** toggle switch.

6. In the **Tag sampling frequency (Hz)** field, specify the frequency (in Hz) at which you need to receive tag values from Kaspersky Industrial CyberSecurity for Networks.

   Indicate `0` in this field if data sampling is not required. *Data sampling* is a method of adjusting a training sample to balance the distribution of classes in the original data set.

7. If you need to recalculate the tag values based on the parameter values specified in the preset file, turn on the **Scale obtained tag values** toggle switch.

   By default, scaling of the received data is disabled.

8. Click the **Save** button.

Kaspersky MLAD receives data from Kaspersky Industrial CyberSecurity for Networks and sends back messages about incident registration.

Configuring the CEF Connector

Kaspersky MLAD uses the CEF Connector to receive data from external sources of events (such as the Industrial Internet of Things, network devices and applications) and to send incident registration messages to an external system.

You can also use the CEF Connector to send information security event logs of Kaspersky MLAD to an external system. Information security event logs are automatically written to the Kaspersky MLAD database.

To receive events from external sources using the CEF Connector, configure the Event Processor service. Before configuring the CEF Connector settings in the Kaspersky MLAD web interface, the IP address and port number to be used for connecting the external event source to the CEF Connector must be specified in the .env file. The settings of the configuration file can be changed only by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

System administrators can configure the CEF Connector.

The CEF Connector does not support a secure connection. If you want to use a secure connection to receive and send data, it is recommended to use additional means to secure the network connection (for example, use a VPN) or use another method to prevent unauthorized access to the communication channel.

To configure the CEF Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **CEF Connector**.

   A list of options appears on the right.

3. If necessary, use the **Receive events for Event Processor service** toggle switch to enable use of the CEF Connector for receiving events from an external system.

4. If you need to send messages about incidents registered by the application to an external system, turn on the **Send registered incidents to SIEM system** toggle switch.

5. To send messages about the events registered by the Event Processor service to an external system, enable the **Send registered events to SIEM system** option.

6. In the **IP address for sending events and incidents to SIEM system** field, specify the IP address for connecting an external system to the CEF Connector and forwarding events processed by the Event Processor service and incidents.

7. In the **Port for sending events and incidents to SIEM system** field, specify the port number for connecting an external system to the CEF Connector and forwarding events processed by the Event Processor service and incidents.

8. If you need to send information security event logs of Kaspersky MLAD to an external system, turn on the **Send information security event logs to Syslog server** toggle switch and do the following:

   a. In the **Transport protocol for sending information security events to Syslog server** drop-down list, select the protocol that you want to use for sending information security event logs.

      Kaspersky MLAD supports the TCP and UDP protocols for sending information security event logs to an external system.

   b. In the **Syslog server address for sending information security events** field, specify the IP address or host name of the external system to which the information security event logs must be sent.

    c. In the **Syslog server port for sending information security events** field, specify the port number of the external system to which the information security event logs must be sent.

9. Click the **Save** button.

Configuring the WebSocket Connector

Kaspersky MLAD uses the WebSocket Connector to receive data and send messages about incident registration via the WebSocket protocol.

> System administrators can configure the WebSocket Connector. The instructions in this section are provided for information purposes.

To configure the WebSocket Connector:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **WebSocket Connector**.

   A list of options appears on the right.

3. In the **WebSocket server web address** field, specify the web address of the WebSocket server that the WebSocket Connector will interact with.

   Enter the web address in the format: `WebSocket protocol://address:port/`.

4. If it is necessary to use a secure connection and a self-signed certificate is installed on the WebSocket server, add the root certificate for the WebSocket server using the **Browse** button under the **CA certificate** setting.

   To delete the certificate file, click the **Clear** icon (🗑). To save the certificate file on your computer, click the **Download** icon (⭳).

5. If it is necessary to use a secure connection and client authentication is enabled on the WebSocket server, do the following:

   - Add the WebSocket client application certificate by using the **Browse** button under the **Client certificate** setting.

   - Add the key to the WebSocket client application certificate by using the **Browse** button under the **Key to client certificate** setting.

   > It is recommended to use a certificate created according to the X.509 standard with a certificate key length of at least 4096 bits.

   To delete the certificate file or certificate key, click the **Clear** icon (🗑) in the corresponding field. To save the certificate file or certificate key on your computer, click the **Download** icon (⭳) in the corresponding field.

6. In the **Data format** drop-down list, select the format to receive data from external systems and send incident alerts.

   The following options are available: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

   The default value of this parameter is `JSONBatch`.

If none of the incident data and alert formats suits you, you can contact Kaspersky Lab experts to add the required format.

7. If you have selected the `Topic` data format, add a configuration file containing the connector settings for this data format using the **Browse** button under the **Connector configuration file** setting.

   To delete the connector configuration file, click the **Clear** icon (🗑). To save the connector configuration file on your computer, click the **Download** icon (⤓).

8. If you need to recalculate the tag values based on the parameter values specified in the preset file, turn on the **Scale obtained tag values** toggle switch.

   By default, scaling of the received data is disabled.

9. To send alerts about the incidents registered in Kaspersky MLAD to a WebSocket server, enable the **Submit incidents** option.

10. Click the **Save** button.

Kaspersky MLAD will receive data and send messages about incident registration via the WebSocket protocol.

Configuring the Event Processor service

Kaspersky MLAD uses the Event Processor service to identify patterns and anomalous sequences of events and patterns. You can configure the settings of the Event Processor service.

If Kaspersky MLAD is restarted, you do not need to re-configure the Event Processor service settings. Kaspersky MLAD restores the Event Processor service state from the database or file in bit format. This restoration process may take several minutes if there is a significantly large number of processed events or registered patterns. Until the state of the Event Processor service is restored in the **Event Processor** section, requests will not be fulfilled, data will not be updated, and data received from the CEF Connector will not be processed. This data is temporarily stored in the system message queue and is processed after the state of the Event Processor service is restored.

The Event Processor service may require a large amount of RAM on the server where Kaspersky MLAD is installed. The amount of RAM usage depends on the rate of the event stream and the volume of events history that is processed. The specific configuration of the Event Processor service also has an effect on the amount of RAM usage.

System administrators can configure the Event Processor service.

To configure the Event Processor service:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters** → **Event Processor**.

   A list of service settings appears on the right.

3. In the **Online mode** section, do the following:

   a. Using the **Browse** button under the setting **Event processor configuration file** field, add the file containing the configuration settings for the Event Processor service.

The Configuration file is created by a qualified technical specialist of the Customer, a Kaspersky Lab employee or a certified integrator.

To delete the configuration file for the Event Processor service, click **Clear** (🗑). To save the configuration file on your computer, click the **Download** icon (⤓).

> Changing the configuration file of the Event Processor service results in a complete loss of the service's data.

b. If you need to process incidents registered by the Anomaly Detector service, turn on the **Process incidents as events** toggle switch.

c. In the **Maximum number of network layers** field, specify the number of layers of the semantic neural network that will be used.

The default number of network layers for event data that is based on a specific structure is ten layers. In most cases, ten layers are enough for the hierarchical presentation of data in the semantic neural network at the core of the Event Processor. To identify patterns of periodic processes that span an extended period of time, you may need to increase the value of the **Maximum number of network layers** parameter.

d. In the **Coefficient defining the permitted dispersion of the pattern duration** field, specify the coefficient used to determine the permissible dispersion of intervals between elements in the same pattern.

If the actual dispersion value is less than or equal to one that is specified, the identified sequences of events will be registered as one pattern.

e. In the **Interval for receiving batch events (sec.)** field, specify the time interval (in seconds) for which the Event Processor service forms an episode from incoming events received for processing.

If the rate of incoming events is approximately 1000 events per second, it is recommended to indicate this value as the interval for receiving new events so that you receive a number of events close to the value indicated in the **Batch size in online mode (number of events)** field during the specified period. If the rate of incoming events is a lot lower than this value, you should adjust the interval for receiving new events to ensure an optimal frequency of event processing.

f. In the **Batch size in online mode (number of events)** field, specify the maximum number of events per episode to be subsequently processed by the Event Processor service.

If the rate of incoming events is approximately 1000 events per second, it is recommended to indicate a value equal to `4096` in this field.

g. In the **Method of saving the state of the Event Processor service** drop-down list, select one of the following options for saving the Event Processor service state:

- **Database table** – Kaspersky MLAD saves the results from processing each episode in the database table.
- **File in bit format** – Kaspersky MLAD saves the state of the Event Processor service according to the frequency defined in the **Component backup frequency** field. The application saves the state of the service to the file specified in the **File containing a backup copy of the component state** field.

> Saving the Event Processor service state to a file in bit format is recommended for debugging and configuring the application settings by Kaspersky employees during the deployment of Kaspersky MLAD.

By default, the Event Processor service saves the results of event stream processing in a database table.

> Changing the way of saving the Event Processor service state results in a complete loss of the service's data.

h. If you select to store the Event Processor service state in a file in bit format, in the **Component backup frequency** field, specify how often (in days, hours, and minutes) to perform a backup of the Event Processor service.

i. If you chose to store the status of the Event Processor service as a bitmap file, add the file that contains a backup copy of the Event Processor service via the **Browse** button under the **File containing a backup copy of the component state** setting.

   This file will be used if you ever need to restore the state of the Event Processor service. The state of the Event Processor service can be restored by Kaspersky experts as part of their extended technical support.

   To delete the file containing a backup copy of the Event Processor service, click **Clear** (🗑). To save the file containing a backup copy of the service on your computer, click the **Download** (⤓) icon.

4. In the **Sleep mode** section, do the following:

   a. In the **Batch size in sleep mode (number of events)** field, specify the number of events for forming an episode in sleep mode.

   The Event Processor service generates episodes based on the history of events received for reprocessing during the time interval specified in the **Events history interval for processing in sleep mode** field.

   b. In the **Send alerts when the monitor is activated in sleep mode** field, select one of the following values:

   - **Send alerts when the monitor is activated by any pattern** – Kaspersky MLAD sends alerts when the monitor is activated in the sleep mode if the patterns are detected in accordance with the specified monitoring criteria. The number of monitor activations is refreshed in the **Event Processor** section on the **Monitoring** tab.

   - **Do not send alerts when the monitor is activated** – Kaspersky MLAD does not send alerts when the monitor is activated in the sleep mode.

   - **Send alerts when the monitor is activated by a new pattern** – Kaspersky MLAD sends alerts when the monitor is activated in the sleep mode if new patterns are detected in accordance with the specified monitoring criteria. The number of monitor activations is refreshed in the **Event Processor** section on the **Monitoring** tab.

   - **Send alerts when the monitor is activated by a previously registered pattern** – Kaspersky MLAD sends alerts when the monitor is activated in the sleep mode if stable patterns are detected in accordance with the specified monitoring criteria. The number of monitor activations is refreshed in the **Event Processor** section on the **Monitoring** tab.

   c. In the **Sleep mode frequency** field, specify how often (in days) and at what time (according to the UTC standard) the Event Processor service goes to the sleep mode to reprocess events.

   It is recommended to specify the time when the event stream is the least intensive as the start time for the sleep mode.

   If the specified sleep time has not yet come on the current day, the Event Processor will go to the sleep mode on that day. If the sleep time has already been missed on the current day, the Event Processor will go to the sleep mode at the specified time after the specified number of days.

   d. In the **Sleep mode duration (HH:MM)** field, specify the time period (in hours and minutes) during which the Event Processor service processes events in the sleep mode.

   e. In the **Events history interval for processing in sleep mode** field, specify the time interval (in days, hours, and minutes) during which the analyzed events must be forwarded for reprocessing in the sleep mode to the Event Processor service.

5. Click the **Save** button.

Configuring the statuses and causes of incidents

Kaspersky MLAD lets you specify the causes of incidents and the statuses of incidents and groups of incidents.

The status of an incident or a group of incidents is a mark about the status of incident analysis performed by an expert. After installation of Kaspersky MLAD, the following statuses of incidents and incident groups are available by default: **Under review**, **Decision pending**, **Instructions issued**, **Problem closed**, **Cause unknown**, **Ignore** and **False positive**.

The incident cause is a mark of the cause of the incident added by an expert based on the results of the incident analysis.

You can add causes and statuses for incidents. The created causes and statuses of incidents will become available for selection in the **Incidents** section. You can also change and delete statuses and causes of incidents.

> System administrators can configure the causes and statuses of incidents.

To add statuses of incidents:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **System parameters** → **Incidents** section.

3. In the **Statuses of incidents** section, click the **Create** button.

   The **Create element** pane will appear on the right.

4. In the **Value, in Russian** field, specify the name of the incident status in Russian.

5. In the **Value, in English** field, specify the name of the incident status in English.

6. In the **Sort** field, indicate the sequence number for which the incident status will be sorted in the **Status** drop-down list in the **Incidents** section.

   The statuses of incidents will be sorted by their names if the sequence numbers of incident statuses coincide.

7. To send incident registration notifications together with the added status and display its indicator in the MSE subsection of the **Monitoring** and **History** sections, select the **Notify about an incident** check box.

8. Click the **Save** button.

To add causes for incidents:

1. In the administrator menu, select **System parameters** → **Incidents**.

2. In the **Causes of incidents** section, click the **Create** button.

The **Create element** pane will appear on the right.

3. In the **Incident cause** field, specify the name of the incident cause.
4. In the **Sort** field, indicate the sequence number for which the incident cause will be sorted in the **Incident cause** drop-down list in the **Incidents** section.

   The causes of incidents will be sorted by their names if the sequence numbers of incident causes coincide.
5. Click the **Save** button.

To change the statuses or causes of incidents:

1. In the administrator menu, select **System parameters** → **Incidents**.
2. To change the parameters of incidents, do one of the following:
   - If you need to change the statuses of incidents or groups of incidents, use the **Statuses of incidents** settings group to select one or more incident statuses and click the **Edit** button.
   - If you need to change the causes of incidents, use the **Causes of incidents** settings group to select one or more incident causes and click the **Edit** button.
3. Make the necessary changes.
4. Click the **Save** button.

To remove statuses or causes of incidents:

1. In the administrator menu, select **System parameters** → **Incidents**.
2. To remove parameters of incidents, do one of the following:
   - If you need to delete the statuses of incidents or groups of incidents, use the **Statuses of incidents** settings group to select one or more incident statuses and click the **Delete** button.
   - If you need to delete the causes of incidents, use the **Causes of incidents** settings group to select one or more incident causes and click the **Delete** button.
3. In the opened window, click **Yes** to confirm deletion.

Kaspersky MLAD will remove information about the incident statuses and causes from the corresponding tables and will remove them from the information about incidents and incident groups in the **Incidents** section for which these incident causes or statuses were selected.

Configuring logging of Kaspersky MLAD services

You can configure the log level for Kaspersky MLAD services to write specific information about the state of the application and display it in the logging system (Grafana). To view how Kaspersky MLAD services are mapped to the names of Docker containers and images, see the Appendix.

System administrators can configure the logging of Kaspersky MLAD services.

To configure the log levels of Kaspersky MLAD services:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **System parameters** → **Logging** section.

   The list of Kaspersky MLAD services will be displayed on the right.

3. If necessary, use the drop-down lists next to the name of the relevant service to change the log level of the service.

   The following log levels are available in Kaspersky MLAD:

   - **Debug** – log all information in the application.
   - **Info** – log basic information about application operations.
   - **General** – log important information about application operations.
   - **Warning** – log errors that occur during operation of the application and log events that could lead to errors in application operations.
   - **Error** – log errors that occur in application operations.
   - **Critical** – log critical errors that occur in application operations.

   The **General** log level is used for most services by default. The **Info** log level is used for the API Server service by default.

4. Click the **Save** button.

Configuring time intervals for displaying data

Kaspersky MLAD lets you specify the time interval (scale) for displaying data on graphs in the **Monitoring**, **History** and **Time slice** sections. After installation of Kaspersky MLAD, the following time intervals are available by default:

- 1, 5, 10, 15, and 30 minutes
- 1, 3, 6, and 12 hours
- 1, 2, 15, and 30 days
- 3 and 6 months
- 1, 2, and 3 years

You can add time intervals for displaying data on graphs. The created time intervals will become available for selection in the **Monitoring**, **History** and **Time slice** sections. You can also edit and delete time intervals.

> System administrators can configure the time intervals for displaying data on charts.

To add time intervals for displaying data:

1. In the lower-left corner of the page, click the ⚙ button.

You will be taken to the administrator menu.

2. Select the **System parameters** → **Graphs** section.
3. In the **Time intervals** settings group, click the **Create** button.

   The **Create element** pane will appear on the right.
4. In the **Time interval (sec.)** field, specify the time interval for which you want to display data on graphs.

   When a time interval is entered, Kaspersky MLAD automatically breaks down the time interval into specific units of time (years, months, weeks, days, hours, minutes, and seconds) in the **Value, in Russian** and **Value, in English** fields.
5. If necessary, change the Russian name of the time interval in the **Value, in Russian** field.
6. If necessary, change the English name of the time interval in the **Value, in English** field.
7. In the **Sort** field, indicate the sequence number for which the time interval will be sorted in the drop-down lists in the **Monitoring**, **History** and **Time slice** section.
8. Click the **Save** button.

To change the time intervals for displaying data:

1. In the administrator menu, select **System parameters** → **Graphs**.
2. In the **Time intervals** settings group, select one or more time intervals and click the **Edit** button.
3. Make the necessary changes.
4. Click the **Save** button.

To delete time intervals for displaying data:

1. In the administrator menu, select **System parameters** → **Graphs**.
2. In the **Time intervals** settings group, select one or more time intervals and click the **Delete** button.
3. In the opened window, click **Yes** to confirm deletion.

Information about the time interval will be deleted from the table.

Configuring how the Kaspersky MLAD main menu is displayed

System administrators can configure settings for displaying the main menu of Kaspersky MLAD.

To configure how the main menu and the administrator menu of Kaspersky MLAD are displayed:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.
2. On the opened page, in the menu on the left, select **System parameters** → **Menu**.

A list of options appears on the right.

3. In the **Availability of main menu items** settings group, use the toggle switch to enable or disable the display of a specific section in the main menu.

4. In the **Availability of administrator menu items** settings group, use the toggle switch to enable or disable the display of a specific section in the administrator menu.

5. Click the **Save** button.

Export and import of Kaspersky MLAD settings

Kaspersky MLAD allows you to export and import configuration files that contain the settings of application services and connectors, as well as security settings, application service logging levels, settings for displaying the application menu and for managing typical statuses and causes of incidents, which are configured through the web interface. This could substantially reduce the time spent on configuring Kaspersky MLAD if you have to re-deploy the application.

> When exporting settings, Kaspersky MLAD does not save to the archive file the passwords specified in the **System parameters** section, as well as the certificate files and certificate file keys uploaded in this section.

> Only system administrators are allowed to export and import configuration files for Kaspersky MLAD services.

To export configuration files from Kaspersky MLAD:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select **System parameters**.

3. Click the **Export** button in the upper part of the opened page.

Kaspersky MLAD configuration files will be saved in an archive named mlad-settings.tar.gz on the local computer.

To upload configuration files to Kaspersky MLAD:

1. In the administrator menu, select **System parameters**.

2. Click the **Import** button in the upper part of the opened page.

3. In the opened window, select the archive file containing the necessary configuration of Kaspersky MLAD parameters.

Kaspersky MLAD configuration files will be uploaded to the application.

Managing assets and tags

> System administrators can manage assets and tags.

Assets and tags are the primary elements of the monitored asset hierarchical structure. The hierarchical structure is displayed as an asset tree.

Observations of the monitored asset are transmitted to Kaspersky MLAD as tags. Based on the values obtained from the created tags, you can perform training and inference of ML models.

In the **Assets** section of the administrator menu, you can view assets and tags that have been created or uploaded to Kaspersky MLAD. Using the plus (⊞) and minus (⊟) signs to the left of the asset names, you can display or hide the asset tree data. You can create assets and tags, and edit tag parameters, such as blocking thresholds of tags or boundaries for displaying tag values on a graph.

Kaspersky MLAD can receive data from assets registered in external systems (for example, Kaspersky Industrial CyberSecurity for Networks). Kaspersky MLAD saves the tags received from external assets in the Time Series Database service. When saving of all tags is enabled, the Time Series Database service also saves IDs and values of unknown tags (not listed in the asset tree). You can compare the current asset tree structure with the structure in the Time Series Database service and add missing tags to the current structure, if necessary.

If Kaspersky MLAD detects unknown tags received from external devices through KICS Connector, these tags will be automatically created in the **KICS** section of the asset tree. The application automatically assigns IDs to tags and fills in the following information received from Kaspersky Industrial CyberSecurity for Networks:

- IDs of the tags
- Names of the tags
- Descriptions of the tags
- Units of measure for the tags
- Names of the assets for which the tags are received

> Kaspersky MLAD is compatible with Kaspersky Industrial CyberSecurity for Networks version 4.0 and later.

You can also delete existing tags, import tags and assets from an XLSX file, or export them to a an XLSX file.

Creating an asset in the asset tree

> System administrators can manage assets and tags.

In Kaspersky MLAD, you can create assets in the asset tree and categorize tags by asset as you see fit. For example, you can create assets for the assets of the monitored asset from which telemetry data is received.

To create a new asset:

1. In the lower-left corner of the page, click the button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the upper part of the page, click the **Create** button.

   The **Create tag** pane opens on the right.

4. In the **Element type** drop-down list, select the **Asset** value.

5. If necessary, click the **Choose icon** button and select an icon for the asset in the opened window.

   You can upload an asset icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the asset icon, click the tag icon and then click **Delete** in the opened window.

6. In the **Asset** drop-down list, select the section of the asset tree within which you want to create the asset.

7. Specify the asset name in the **Name** field.

8. In the **Description** field, provide a description for the asset.

9. Select the type of asset from the **Asset type** drop-down list.

   If you have uploaded the configuration of assets and tags to Kaspersky MLAD, you can select one of the asset types defined in the configuration file. Asset types are specified in the **directory_types** tab of the configuration file.

10. If you have selected one of the asset types defined in the imported configuration file, specify values for the special parameters of the assets.

    The names of special parameters are specified in the **directory_types** tab of the configuration file.

11. Click the **Save** button.

The asset will be created. If necessary, you can change the position of an asset in the tree.

You can also create nested assets in the asset tree.

To create an asset using the asset tree:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the asset tree, next to the name of the section to which you want to add the asset, open the vertical menu **...** and select **Add asset**.

   The **Create asset** pane opens on the right.

4. If necessary, click the **Choose icon** button and select an icon for the asset in the opened window.

   You can upload an asset icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the asset icon, click the tag icon and then click **Delete** in the opened window.

5. Specify the asset name in the **Name** field.

6. In the **Description** field, provide a description for the asset.

7. Select the type of asset from the **Asset type** drop-down list.

   If you have uploaded the configuration of assets and tags to Kaspersky MLAD, you can select one of the asset types defined in the configuration file. Asset types are specified in the **directory_types** tab of the configuration file.

8. If you have selected one of the asset types defined in the imported configuration file, specify values for the special parameters of the assets.

   The names of special parameters are specified in the **directory_types** tab of the configuration file.

9. Click the **Save** button.

The asset will be created. If necessary, you can change the position of an asset in the tree.

Changing the parameters of an asset in the asset tree

System administrators can manage assets and tags.

You can edit the settings of previously created assets.

To edit the settings of an asset in the asset tree:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the asset tree, next to the name of the asset whose settings you want to change, open the vertical menu **...** and select **Edit asset**.

   The **Edit asset** pane opens on the right.

4. If you need to change the icon of the asset, click the **Choose icon** button and select an icon for the asset in the opened window.

   You can upload an asset icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the asset icon, click the tag icon and then click **Delete** in the opened window.

5. In the **Asset** drop-down list, select the section of the asset tree to which you want to assign the asset.

   The asset subsections and their tags are moved to the new asset.

6. In the **Name** field, specify a new name for the asset.

7. In the **Description** field, specify a new description for the asset.

8. Select the type of asset from the **Asset type** drop-down list.

   If you have uploaded the configuration of tags and assets to Kaspersky MLAD, you can select one of the asset types defined in the configuration file. Asset types are specified in the **directory_types** tab of the configuration file.

9. If you have selected one of the asset types defined in the imported configuration file, specify values for the special parameters of the asset.

   The names of special parameters are specified in the **directory_types** tab of the configuration file.

10. Click the **Save** button.

The asset will be modified. If necessary, you can change the position of an asset in the tree.

Create tag

> System administrators can manage assets and tags.

In Kaspersky MLAD, you can create new tags to describe data received from the monitored asset (source tags) or from the Stream Processor service.

To create a new tag:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the upper part of the page, click the **Create** button.

   The **Create tag** pane opens on the right.

4. In the **Element type** drop-down list, select **Tag**.

5. If necessary, click the **Choose icon** button and select an icon for the tag in the opened window.

   You can upload the tag icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the tag icon, click the tag icon and then click **Delete** in the opened window.

6. In the **Asset** drop-down list, select the section of the asset tree to which you want to assign the created tag.

   Assets in the asset tree must be preloaded or created manually.

7. Specify the unique tag name in the **Name** field. If you want to receive tag values from an external system, specify the tag name in the external system.

8. Enter a description for the tag in the **Description** field.

9. If necessary, specify an alternative name for the tag in the **Alternative name** field.

10. Enter the unique numerical identifier of the tag in the **ID** field.

11. In the **Dimension** field, specify the measurement units for the tag (for example % or mPa).

12. In the **X**, **Y**, and **Z** fields, specify the spatial coordinates for the location of the monitored asset's sensor.

    You can use an arbitrary point as the origin of the coordinate system.

    You can use sensor coordinates to calculate tag values when creating a preset and displaying them on the graph in the **Time slice** section.

13. In the **Blocking threshold** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

    These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower blocking threshold, the Limit Detector registers an incident.

    If the **Always display blocking threshold** option is enabled, the vertical scale of the graph will be defined by threshold lines drawn at the lower and upper boundaries of the tag graph, provided that the tag values are within the specified range. If the tag values go beyond the specified thresholds, the vertical scale will be automatically changed to display the tag values exceeding the limits.

14. In the **Alarm threshold**, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of the tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

15. In the **Measurement confidence thresholds** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds for physically possible tag values.

16. In the **Display boundaries** section, in the **Lower** and **Upper** fields, specify the lower and upper boundaries for displaying tag values on graphs.

    If tag values go beyond the defined boundaries, they will not be displayed on the tag graph. The permissible boundaries for displaying tag values take priority over the display of blocking thresholds, even if the **Always display blocking threshold** function is enabled.

17. In the **External system asset** field, specify the name of the asset created in the external system, for which you need to receive tags.

18. In the **Comment** field, enter a brief comment for the tag.

19. If you want to add additional horizontal threshold lines for this tag on the charts in the **Monitoring** and **History** sections, do the following:

    a. Click the **Add line** button.

    b. In the **Threshold value** field that appears, specify the value that you want to display on the charts.

    c. In the **Line color** field, select the color in which the threshold line will be displayed on the charts.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

20. Click the **Save** button.

The new tag appears in the **Tags** group of the asset tree. The **Tags** group is created automatically and displayed as part of the selected section of the asset tree. If necessary, you can change the position of tags in the tree.

Adding a tag to an asset

> System administrators can manage assets and tags.

In Kaspersky MLAD, you can add tags to created assets.

To add a tag to an asset:

1. In the lower-left corner of the page, click the ⚙ button.

You will be taken to the administrator menu.

2. Select the **Assets** section.
3. In the asset tree, next to the section to which you want to add a tag, open the vertical menu **...** and select **Add tag**.

   The **Create tag** pane opens on the right.
4. If necessary, click the **Choose icon** button and select an icon for the tag in the opened window.

   You can upload the tag icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the tag icon, click the tag icon and then click **Delete** in the opened window.
5. Specify the unique tag name in the **Name** field. If you want to receive tag values from an external system, specify the tag name in the external system.
6. Enter a description for the tag in the **Description** field.
7. If necessary, specify an alternative name for the tag in the **Alternative name** field.
8. Enter the unique numerical identifier of the tag in the **ID** field.
9. In the **Dimension** field, specify the measurement units for the tag (for example % or mPa).
10. In the **X**, **Y**, and **Z** fields, specify the spatial coordinates for the location of the monitored asset's sensor.

    You can use an arbitrary point as the origin of the coordinate system.

    You can use sensor coordinates to calculate tag values when creating a preset and displaying them on the graph in the **Time slice** section.
11. In the **Blocking threshold** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

    These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower blocking threshold, the Limit Detector registers an incident.

    If the **Always display blocking threshold** option is enabled, the vertical scale of the graph will be defined by threshold lines drawn at the lower and upper boundaries of the tag graph, provided that the tag values are within the specified range. If the tag values go beyond the specified thresholds, the vertical scale will be automatically changed to display the tag values exceeding the limits.
12. In the **Alarm threshold**, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of the tag values, upon reaching which it is necessary for the ICS to take emergency response measures.
13. In the **Measurement confidence thresholds** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds for physically possible tag values.
14. In the **Display boundaries** section, in the **Lower** and **Upper** fields, specify the lower and upper boundaries for displaying tag values on graphs.

    If tag values go beyond the defined boundaries, they will not be displayed on the tag graph. The permissible boundaries for displaying tag values take priority over the display of blocking thresholds, even if the **Always display blocking threshold** function is enabled.

    In the **External system asset** field, specify the name of the asset created in the external system, for which you need to receive tags.
15. In the **Comment** field, enter a brief comment for the tag.

16. If you want to add additional horizontal threshold lines for this tag on the charts in the **Monitoring** and **History** sections, do the following:

    a. Click the **Add line** button.

    b. In the **Threshold value** field that appears, specify the value that you want to display on the charts.

    c. In the **Line color** field, select the color in which the threshold line will be displayed on the charts.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

17. Click the **Save** button.

The new tag appears in the **Tags** group of the asset tree. The **Tags** group is created automatically and displayed as part of the selected section of the asset tree. If necessary, you can change the position of tags in the tree.

Editing a tag

System administrators can manage assets and tags.

You can edit previously created tags.

To edit a tag:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

   In the asset tree, next to the name of the tag that you want to change, open the vertical menu **...** and select **Edit tag**.

   You can show or hide the data in the asset tree by using the plus (⊞) and minus (⊟) icons to the left of the asset names.

   The **Edit tag** pane opens on the right. In the upper part of the pane that opens, the number of ML models that use the selected tag is displayed.

3. If you need to change the icon of the tag, click the **Choose icon** button and select an icon for the tag in the opened window.

   You can upload the tag icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you need to delete the tag icon, click the tag icon and then click **Delete** in the opened window.

4. In the **Asset** drop-down list, select the new asset to which you want to assign the selected tag.

   Specify the new name of the tag in the **Name** field. If you want to receive tag values from an external system, specify the tag name in the external system.

   Kaspersky MLAD periodically verifies information about tags received from Kaspersky Industrial CyberSecurity for Networks. If the tag name was changed manually, the application automatically updates the tag name to match the tag name in Kaspersky Industrial CyberSecurity for Networks after the next scan.

5. Enter a new description for the tag in the **Description** field.

6. If necessary, specify an alternative name for the tag in the **Alternative name** field.

7. In the **Dimension** field, specify new units of measure for the tag (for example, % or mPa).

8. In the **X**, **Y**, and **Z** fields, specify the spatial coordinates for the location of the monitored asset's sensor.

   You can use an arbitrary point as the origin of the coordinate system.

   You can use sensor coordinates to calculate tag values when creating a preset and displaying them on the graph in the **Time slice** section.

9. In the **Blocking threshold** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

   These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower blocking threshold, the Limit Detector registers an incident.

   If the **Always display blocking threshold** option is enabled, the vertical scale of the graph will be defined by threshold lines drawn at the lower and upper boundaries of the tag graph, provided that the tag values are within the specified range. If the tag values go beyond the specified thresholds, the vertical scale will be automatically changed to display the tag values exceeding the limits.

10. In the **Alarm threshold**, in the **Lower** and **Upper** fields, specify the lower and upper thresholds of the tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

11. In the **Measurement confidence thresholds** block, in the **Lower** and **Upper** fields, specify the lower and upper thresholds for physically possible tag values.

12. In the **Display boundaries** section, in the **Lower** and **Upper** fields, specify the lower and upper boundaries for displaying tag values on graphs.

    If tag values go beyond the defined boundaries, they will not be displayed on the tag graph. The permissible boundaries for displaying tag values take priority over the display of blocking thresholds, even if the **Always display blocking threshold** function is enabled.

    In the **External system asset** field, specify the name of the asset created in the external system, for which you need to receive tags.

    Kaspersky MLAD periodically verifies information about tags received from Kaspersky Industrial CyberSecurity for Networks. If information about the tag asset was changed manually, the application automatically updates the information about the asset according to the asset name in Kaspersky Industrial CyberSecurity for Networks after the next scan.

13. In the **Comment** field, enter a brief comment for the tag.

14. If you want to add additional horizontal threshold lines for this tag on the charts in the **Monitoring** and **History** sections, do the following:

    a. Click the **Add line** button.

    b. In the **Threshold value** field that appears, specify the value that you want to display on the charts.

    c. In the **Line color** field, select the color in which you want the threshold line to be displayed on the charts in the **Monitoring** and **History** sections.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

15. Click the **Save** button.

If necessary, you can change the position of tags in the tree.

Moving assets and tags

System administrators can manage assets and tags.

You can move assets and/or tags within the asset tree. All assets and tags that are part of the selected asset will be moved.

To move an asset and/or tag:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the asset tree, select the check boxes next to the names of the assets and/or tags that you want to move.

4. In the upper part of the page, click the **Move** button.

   The **Moving tags** pane opens on the right.

5. In the **Asset** drop-down list, select the asset to which you want to transfer the selected assets and/or tags.

6. Click the **Save** button.

The modified asset tree appears in the **Assets** section.

You can also change the location of assets and tags in the tree using the dots (⠿) to the left of the name of the required asset or tag. To do this, click and hold the dots (⠿) to the left of the relevant asset or tag and drag the relevant asset or tag up or down in the tree.

Deleting an asset or tag

System administrators can manage assets and tags.

You can delete previously created assets and/or tags from the asset tree if the selected tags or tags associated with the selected asset are not used by ML models.

To delete a tag:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. Perform one of the following actions:

   - In the asset tree, select the check box next to the name of the tag that you want to delete and click the **Delete** button at the top of the page.

- In the vertical menu **...** to the right of the relevant tag, click the **Delete tag** button.

4. In the window that opens, confirm the deletion of the tag.

To delete an asset:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. Perform one of the following actions:

   - In the asset tree, select the check box next to the name of the asset that you want to delete and click the **Delete** button at the top of the page.

   - In the vertical menu **...** to the right of the relevant asset, click the **Delete asset** button.

4. In the window that opens, confirm the deletion of the asset.

To remove one or more assets and/or tags:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the asset tree, select the check boxes next to the names of the assets and/or tags.

   If you need to remove one or more tags from an asset, expand the corresponding section of the asset tree by clicking the plus sign (⊞), and select the relevant tags.

4. Click the **Delete** button in the upper part of the page.

5. In the window that opens, confirm the removal of assets and/or tags.

If the selected assets and/or tags are not used by ML models, a check mark icon (✓) is displayed in the window opposite the line **Checking links between tags and loaded models**. The selected tags will be permanently deleted from Kaspersky MLAD.

If the selected assets and/or tags are used by ML models, a cross icon (⊗) is displayed in the window opposite the line **Checking links between tags and loaded models**. In this case, you cannot delete the selected assets and/or tags. To delete assets and/or tags, you must delete the ML models in which they are used.

Checking the current structure of tags

System administrators can manage assets and tags.

Kaspersky MLAD saves the tags received from external assets in the Time Series Database service. When unknown tags are received via KICS Connector, the application also automatically creates these tags in the **KICS** asset tree section.

Kaspersky MLAD allows you to compare the current tag structure displayed in the asset tree and used for a monitored asset to the one saved for this monitored asset in the Time Series Database service. Kaspersky MLAD detects tags that were received from external assets, but are missing in the current tag structure and are not used for the monitored asset. If necessary, you can add these tags to the current tag structure.

To compare the current tag structure with the structure in the Time Series Database service:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. In the upper part of the page, click the **Check tags** button.

   The current tag structure used for the monitored asset is compared with the tag structure stored in the Time Series Database service. The comparison result is displayed in the upper part of the page.

   If missing tags are detected, Kaspersky MLAD displays a list of these tags with the names in the **Tag <tag ID>** format.

4. To add missing tags, do the following:

   a. For each detected tag, in the **Asset** field select the asset to which you want to assign the tag.

   b. Click the **Add** button.

   Kaspersky MLAD will add tags to the asset tree. Only the IDs, names in the **Tag <tag ID>** format, and the assets to which the tags are assigned are specified for these tags. If necessary, you can change the added tags.

Uploading tag and asset configuration to the system

Tag and asset configuration is created while deploying Kaspersky MLAD and building an ML model. Tag and asset configuration is provided in XLSX file format.

System administrators can manage assets and tags.

To upload tag and asset configuration to Kaspersky MLAD:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. Click the **Import** button.

   The **Hierarchical structure import** pane opens on the right.

4. In the **File import** field, add an XLSX file containing the required configuration of assets and hierarchical structure tags.

   To delete the asset and tag configuration file, click the trash bin icon (🗑).

5. In the **Asset** drop-down list, select the section of the asset tree to which you want to load the configuration of assets and tags from a file.

6. In the **Import mode** drop-down list, select one of the following values:

   - **Add and update**. Kaspersky MLAD will add new assets and tags from the configuration file and update information about previously created and/or imported assets and tags within the selected section.

   - **Only update**. Kaspersky MLAD will update information about previously created and/or imported assets and tags within the selected section.

   - **Overwrite**. Kaspersky MLAD will delete previously created and/or imported assets and tags from the selected section and create new assets and tags from the configuration file.

7. If you want all assets and tags from the configuration file to be treated as new occurrences, enable the **Treat all elements as new** check box.

   You can use this toggle switch to upload assets that are duplicated in different sections of the asset tree in **Add and update** import mode. However, you cannot load tags with names that match the names of previously created and/or loaded tags.

8. Click the **Save** button.

Tag and asset configuration will be uploaded to Kaspersky MLAD. The assets and tags are displayed as an asset tree.

Saving tag and asset configuration to a file

> System administrators can manage assets and tags.

You can save the structure of tags to a file in XLSX format for subsequent use. The hierarchical asset structure will be saved together with the tag structure in the file.

To save tag and asset configuration to a XLSX file:

1. In the lower-left corner of the page, click the ⚙ button.

   You will be taken to the administrator menu.

2. Select the **Assets** section.

3. Click the **Export** button.

The asset and tag configuration will be saved to a file named mlad_structure.xlsx (see the example in the Appendix).

Working with the main menu

This section contains a description of user tasks performed in the main menu of the application.

Access to application functions in the main menu depends on the role assigned to the user account. Users with the system administrator role have access to all functions of the application.

Scenario: working with Kaspersky MLAD

This section describes the actions that can be taken by a user when working in the main menu of Kaspersky MLAD.

The scenario for working with the application consists of the following steps:

1. **Creating presets to monitor the section of the protected facility**

   For quick and more convenient access to necessary data, it is recommended to create presets that include tags corresponding to units of the industrial plant. If necessary, you can modify existing presets.

2. **Viewing historical data**

   Go to the **History** section to view historical data of process parameters, generated predictions and identified incidents resulting from Kaspersky MLAD processing. Select the relevant preset and specify the date and time interval for viewing the data. Use the navigation to view historical data.

3. **Monitoring in online mode**

   To view the received values of process parameters, their predicted values, and errors in the online mode, go to the **Monitoring** section. Select the relevant preset and time interval to display the incoming data.

4. **Viewing data in the Time slice section**

   To view the values of the process parameters received from the monitored asset's sensors at a certain point in time, go to the **Time slice** section. Select the relevant preset and specify the date and time interval for viewing the data. Use the navigation to view data.

5. **Working with incidents**

   Go to the **Incidents** section and view information about the registered incidents. Analyze the incidents and add expert opinions or comments where you can indicate if the registered incidents are anomalies.

   If you are subscribed to incident notifications, you will receive an email message when an abnormal situation arises. The message will indicate the date and time when the incident began and will provide a link you can use to go to the **History** section.

6. **Working with events and patterns**

   View the events and patterns detected by the Event Processor in the **Event Processor** section. Create monitors to monitor specific events, patterns, and event parameter values.

Viewing summary data in the Dashboard section

The **Dashboard** section provides summary information on the number of tags and events received by Kaspersky MLAD, registered incidents, and the status of services.

The information on the page is divided into the following blocks:

- **Incoming data** is a graph that displays the number of tags and events received by Kaspersky MLAD. You can enable or disable the display of incoming tags and events on the graph by clicking the corresponding data signature legend under the graph. The left scale of the graph displays the range for the number of incoming tags per second. The right scale of the graph displays the range for the number of incoming events per second.

- **Latest incidents** is a table that contains information about the latest registered incidents.

  - **ID** refers to the ID of the registered incident.

  - **Date and time** refers to the date and time when the incident occurred.

  - **Detector** is the name of the detector that registered the incident.

  - **Top tag** refers to the name of a technological process parameter for which the incident is registered.

  Clicking the plus (+) next to the incident in the incidents table opens a window with the technical specification of the selected incident and tag:

  - **Incident** is a section containing information about the incident:

    - **Model name** refers to the name of the utilized ML model.

    - **Model branch** is the name of the ML model branch being used.

    - **Detector** is the name of the detector that registered the incident.

    - **MSE value** is the value of the individual mean square error.

    - **Threshold value** refers to the MSE threshold value for the ML model branch in use at the time of incident registration.

  - **Top tag** is the section containing information about the tag for which the incident is registered:

    - **Top tag name (top tag ID)** is the name and ID of the tag whose behavior invoked registration of the incident.

    - **Top tag value** is the value of the top tag registered when the incident occurred.

    - **Blocking threshold** refer to the thresholds of the top tag values, upon reaching which it is necessary for the ICS to take emergency response measures.

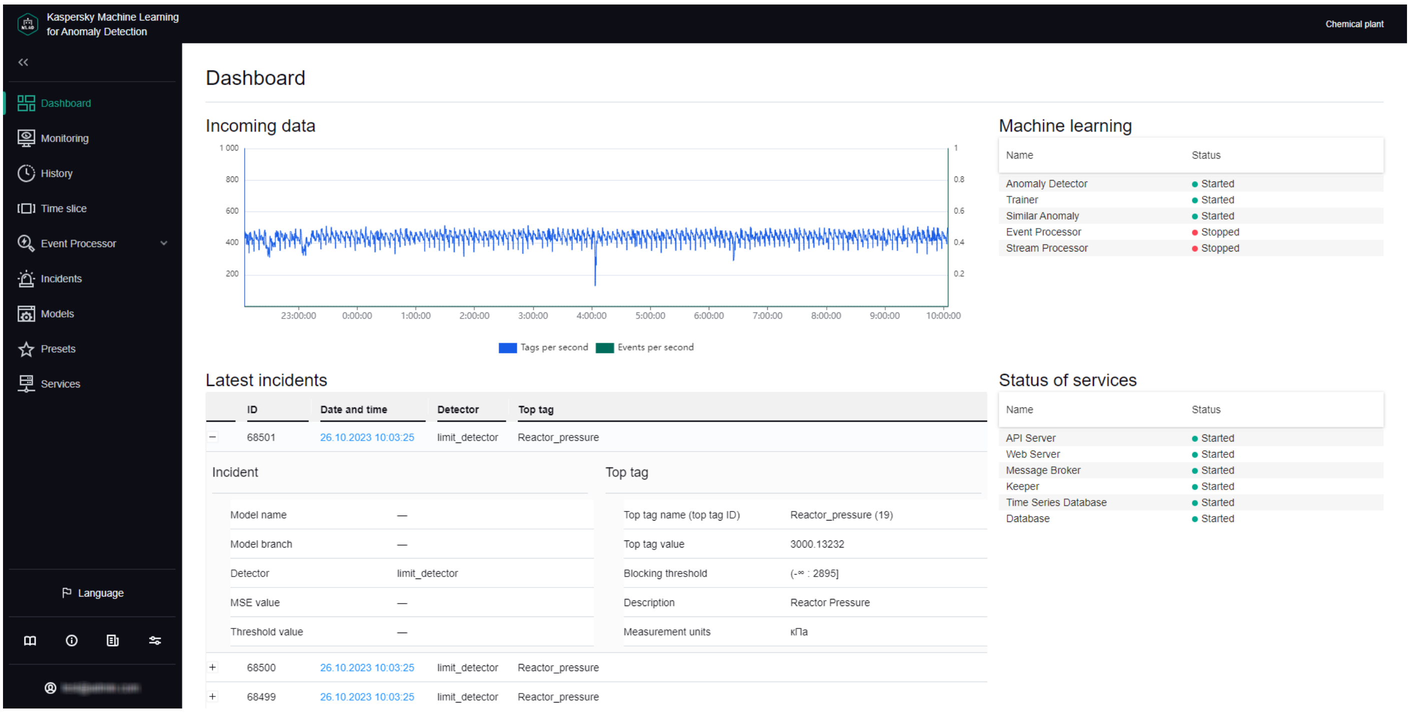
    - **Description** refers to a description of the top tag.

    - **Measurement units** refer to the units for measuring the top tag values.

- **Machine learning** is a table that displays the status of services used for operation and training of the ML model, and the name of the active ML model.

- **Status of services** is a table that displays the status of each service.

You can proceed to the History section from the **Dashboard** section by clicking the date and time of an incident in the **Latest incidents** table. The **History** section displays detailed information about the incidents registered by Kaspersky MLAD.



Dashboard

Incoming data

Machine learning

Name	Status
Anomaly Detector	● Started
Trainer	● Started
Similar Anomaly	● Started
Event Processor	● Stopped
Stream Processor	● Stopped

Latest incidents

	ID	Date and time	Detector	Top tag
−	68501	26.10.2023 10:03:25	limit_detector	Reactor_pressure

Incident

Model name	—
Model branch	—
Detector	limit_detector
MSE value	—
Threshold value	—

Top tag

Top tag name (top tag ID)	Reactor_pressure (19)
Top tag value	3000.13232
Blocking threshold	(-∞ : 2895]
Description	Reactor Pressure
Measurement units	кПа

	ID	Date and time	Detector	Top tag
+	68500	26.10.2023 10:03:25	limit_detector	Reactor_pressure
+	68499	26.10.2023 10:03:25	limit_detector	Reactor_pressure

Status of services

Name	Status
API Server	● Started
Web Server	● Started
Message Broker	● Started
Keeper	● Started
Time Series Database	● Started
Database	● Started

Dashboard section

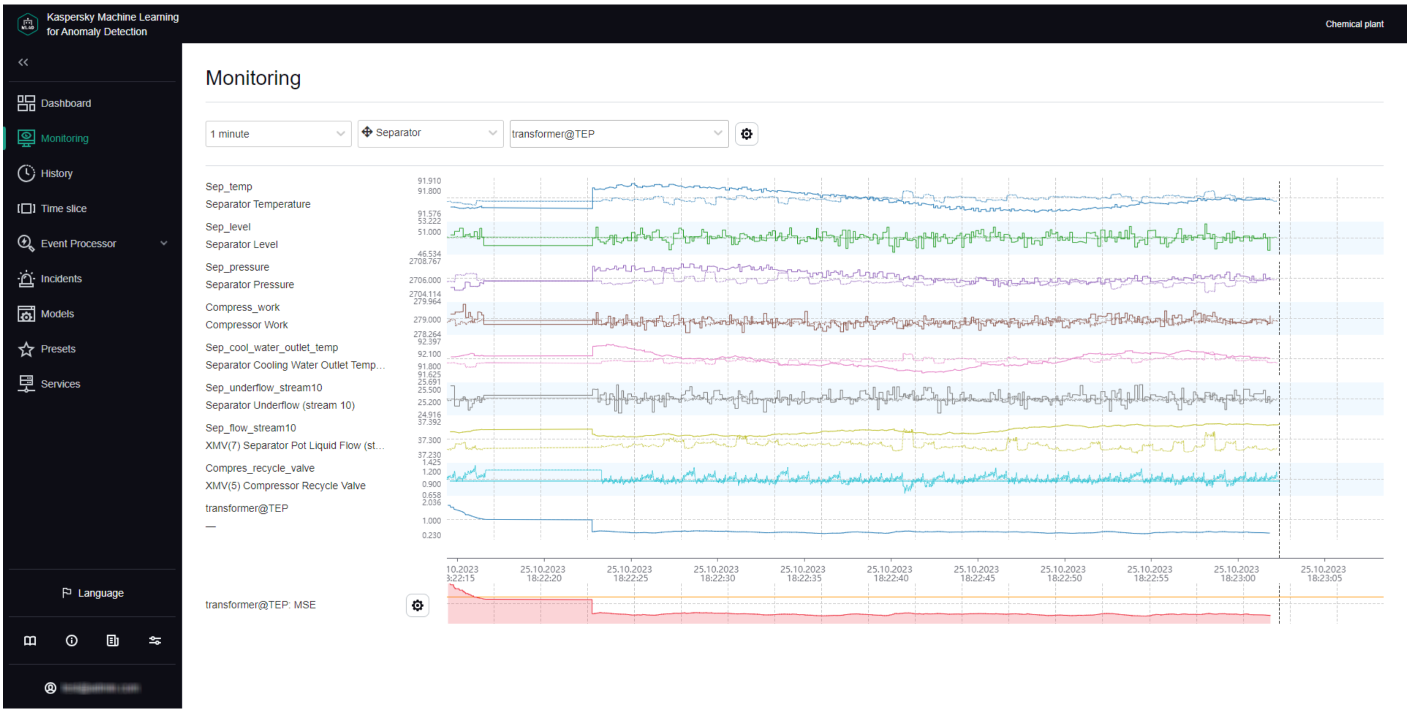
Viewing incoming data in the Monitoring section

In the **Monitoring** section, you can view the real-time values of the tags included in the preset and their predicted values. You can view data on relevant tags by selecting the necessary preset from the drop-down list. This list includes presets that can be created in the **Presets** section. For each tag included in the selected preset, the incoming values are displayed as a graph. You can customize the display of graphs and select a branch of a specific ML model to view the operating results of this branch. For example, you can view the tag values predicted by the Forecaster Detector and their errors, or the values obtained as a result of the work of diagnostic rules.

The lower part of the page contains a section displaying the *cumulative mean square error* (also referred to as the "MSE" or "cumulative error"), and the number of registered incidents (color-coded dot indicators). The orange line shows the MSE threshold, above which Kaspersky MLAD registers an incident.

Depending on the selected time scale and the density of incidents, one dot indicator may correspond to one or multiple closely-spaced incidents that were registered by one or multiple different detectors. The color of dot indicators corresponds to the color of the ML model branch that was used to register the incident. Special colors are reserved for dot indicators that correspond to a group of incidents registered by different branches and for incidents registered by the Limit Detector.

There will be no MSE error value for incidents logged by the Rule Detector. When analyzing these incidents, pay attention to the rule triggering marker (color-coded dot indicator) below the MSE graph for the selected ML model branch.



Monitoring section

Viewing data for a specific preset in the Monitoring section

Kaspersky MLAD allows you to select presets for which real-time data is displayed.

To view incoming data for a specific preset in real time:

1. In the main menu, select the **Monitoring** section.
2. On the opened page, select the relevant preset from the **Preset** drop-down list.

   The page displays graphs for tags that are included in the selected preset.

If necessary, you can change the time interval for displaying data, customize the display of graphs, or select a specific branch of the ML model. You can also change which tags are displayed by editing the preset.

Selecting a specific branch of the ML model in the Monitoring section

In the **Monitoring** section, you can view in real time the incoming values of tags included in the preset, their predicted values, and MSEs.

If the ML model used for a monitored asset has several branches for processing and predicting data, Kaspersky MLAD lets you select a specific branch of the ML model to display the operating results of the corresponding model element:

- For an ML model branch based on the Forecaster Detector, operating results are displayed as predicted values for specific tags, individual errors in the prediction of specific tags, and cumulative MSE and dot indicators of incidents registered by the detector.
- For an ML model branch based on the Rule Detector, operating results are presented as values obtained as a result of the work of diagnostic rules and dot indicators of incidents.

- An ML model branch is not created for the Limit Detector. The dot indicators of incidents registered using this detector are displayed if use of the Limit Detector is enabled and the display of indicators for all tags is enabled.

> To display the predicted values of a tag on graphs in the **Monitoring** section, and to display the values obtained as a result of the work of diagnostic rules, you must customize the display of graphs.

To view the operating results of a specific ML model branch:

1. In the main menu, select the **Monitoring** section.
2. On the opened page, in the **Model branch** drop-down list, select the check boxes next to the relevant branches of the ML model.

   The names of the selected branches are displayed in the field.

   > The branches belonging to the currently used ML model are located in the upper part of the list. The lower part of the list displays branches of other currently unused ML models that were uploaded to Kaspersky MLAD. An ML model branch is displayed in the drop-down list only after Kaspersky MLAD receives data that resulted from operations of the specific branch.

   The graphs of the selected preset will display the predicted values of tags or the values obtained as a result of the work of diagnostic rules depending on the type of detector in the selected ML model branch.

   If you need to hide the display of operating results from previously selected ML model branches, clear the check boxes next to these branches (however, one of the branches must remain active for graphs to be displayed in the **Monitoring** section).
3. If you need to display the MSE received as a result of data processing by a specific ML model branch:

   a. Click the settings button ⚙ below the tag graphs on the left side of the page.

   b. In the **MSE graph display settings** pane that appears on the right, select the branch from the **Model branch** drop-down list. You can select only one ML model branch from the list.

   c. Click the **Close** button.

The MSE graph displays the MSE values for the selected branch of the ML model. The lower part of the graph displays the dot indicators of incidents that were registered by the selected ML model branches. If the display of indicators for all tags is enabled, the dot indicators of incidents that were registered by all ML model branches will be displayed.

Selecting a time interval in the Monitoring section

Kaspersky MLAD lets you select the time interval (scale) for displaying incoming data.

To select a time interval:

1. In the main menu, select the **Monitoring** section.
2. On the opened page, select the necessary time interval from the drop-down list. The following values are available by default:

    - 1, 5, 10, 15, and 30 minutes
    - 1, 3, 6, and 12 hours
    - 1, 2, 15, and 30 days
    - 3 and 6 months
    - 1, 2, and 3 years

    If necessary, the system administrator can create, edit, or delete time intervals.

   The page will display graphs of the defined preset for the selected time interval.

Configuring how graphs are displayed in the Monitoring section

Kaspersky MLAD lets you configure how the graphs of presets are displayed in the **Monitoring** section.

To configure the display settings for preset graphs:

1. In the main menu, select the **Monitoring** section.
2. On the opened page, click the settings button ⚙ in the upper part of the screen.

   The **Graph display settings** pane will appear on the right.
3. In the **Graph height** drop-down list, select one of the following values: 55 px, 110 px, 145 px, 190 px.

   By default, the **Graph height** parameter is set to 55 px.
4. In the **To go to the History section, use** drop-down list, select the preset whose graphs should be displayed by default when you navigate to the **History** section.
5. If necessary, move the **Show observation graphs in selected color** toggle button to enable the display of tag observation graphs in a specific color, and select the color in the **Color of observation graphs** field.
6. If necessary, use the **Show prediction graphs in selected color** toggle switch to enable the display of tag prediction graphs in a specific color, and select the color in the **Color of prediction graphs** field.
7. If necessary, use the **Tag description and name** toggle switch to enable display of the tag description and name on graphs.
8. If necessary, use the **Predicted tag value** toggle switch to enable the display of the predicted tag value and values obtained as a result of the work of diagnostic rules on graphs.
9. If necessary, use the **Personal tag error** toggle switch to enable display of the personal tag error on graphs.
10. If necessary, use the **Display indicators for all incidents** toggle switch to enable display of the dot indicators for incidents registered by all ML model branches.

    If this mode is disabled, only the dot indicators for incidents that were registered by the selected ML model branches will be shown.
11. If you need the graphs to display the defined technical limits for a tag:

    a. Turn on the **Blocking threshold** toggle switch.

b. If you need to always display the defined technical limits, turn on the **Always display blocking threshold** toggle switch.

If this mode is disabled, the technical limits will be displayed only if the tag value has reached the corresponding limit in the graph area displayed on the screen.

12. If necessary, use the **Additional threshold lines** toggle switch to enable the display of additional threshold lines on the graph.

13. Click the **Close** button to return to viewing graphs in the **Monitoring** section.

The defined settings for displaying preset graphs in the **Monitoring** section will be applied.

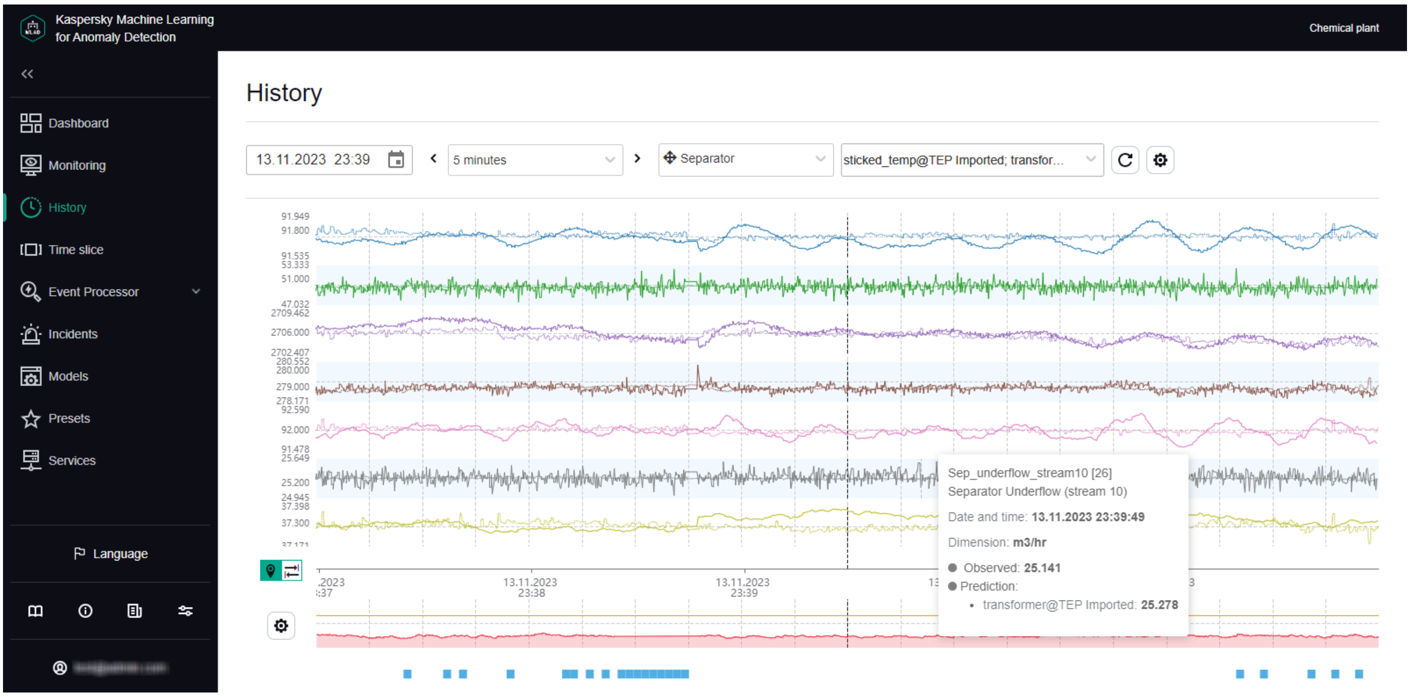
Viewing data in the History section

The **History** section provides access to the history of incoming data, the results of data processing by Kaspersky MLAD, generated predictions, and registered incidents. You can select the necessary preset in the drop-down list. This list includes presets that can be created in the **Presets** section. For each tag included in the selected preset, the incoming values are displayed as a graph. You can customize the display of graphs, select a time interval for viewing data, and select a branch of a specific ML model to view the operating results of this branch. For example, you can view the tag values predicted by the Forecaster Detector and their errors, or the values obtained as a result of the work of diagnostic rules.

The lower part of the page contains a section displaying the *cumulative mean square error* (also referred to as the "MSE" or "cumulative error"), and the number of registered incidents (color-coded dot indicators). The orange line shows the MSE threshold, above which Kaspersky MLAD registers an incident.

Depending on the selected time scale and the density of incidents, one dot indicator may correspond to one or multiple closely-spaced incidents that were registered by one or multiple different detectors. The color of dot indicators corresponds to the color of the ML model branch that was used to register the incident. Special colors are reserved for dot indicators that correspond to a group of incidents registered by different branches and for incidents registered by the Limit Detector.

There will be no MSE error value for incidents logged by the Rule Detector. When analyzing these incidents, pay attention to the rule triggering marker (color-coded dot indicator) below the MSE graph for the selected ML model branch.



13.11.2023 23:39

5 minutes

Separator

sticked_temp@TEP Imported; transfor...

Sep_underflow_stream10 [26]
Separator Underflow (stream 10)

Date and time: **13.11.2023 23:39:49**

Dimension: **m3/hr**

● Observed: **25.141**
● Prediction:
- transformer@TEP Imported: **25.278**

Viewing historical data for a specific preset

Kaspersky MLAD allows you to select custom presets for which historical data is displayed. You can also view information about the Tags for event #N dynamic preset if you go to the **History** section from the **Incidents** section by clicking the incident registration date. The Tags for event #N dynamic preset contains tags that had the greatest influence on the generation of a registered incident.

To view historical data for a specific preset:

1. In the main menu, select the **History** section.
2. On the opened page, select the relevant preset from the **Preset** drop-down list.

   The page displays graphs for tags that are included in the selected preset.

You can use the time navigation function to view the entire history of data. If necessary, you can change the date and time interval. You can also change the composition of tags in a preset, create a new preset, or select a specific branch of the ML model.

Selecting a specific branch of the ML model in the History section

The **History** section provides access to the history of incoming data, the results of data processing by Kaspersky MLAD, generated predictions, and registered incidents.

If the ML model used for a monitored asset has several elements for processing data, Kaspersky MLAD lets you select a specific branch of the ML model to display the operating results of the corresponding model element:

- For an ML model branch based on the Forecaster Detector, operating results are displayed as predicted values for specific tags, individual errors in the prediction of specific tags, and cumulative MSE and dot indicators of incidents registered by the detector.
- For an ML model branch based on the Rule Detector, operating results are presented as values obtained as a result of the work of diagnostic rules and dot indicators of incidents.
- An ML model branch is not created for the Limit Detector. The dot indicators of incidents registered using this detector are displayed if use of the Limit Detector is enabled and the display of indicators for all tags is enabled.

> To display the predicted values of a tag on graphs in the **History** section, and to display the values obtained as a result of the work of diagnostic rules, you must customize the display of graphs.

To view the operating results of a specific ML model branch:

1. In the main menu, select the **History** section.
2. On the opened page, in the **Model branch** drop-down list, select the check boxes next to the relevant branches of the ML model.

   The names of the selected branches are displayed in the field.

> The branches belonging to the currently used ML model are located in the upper part of the list. The lower part of the list displays branches of other currently unused ML models that were uploaded to Kaspersky MLAD. An ML model branch is displayed in the drop-down list only after Kaspersky MLAD receives data that resulted from operations of the specific branch.

The graphs of the selected preset will display the predicted values of tags or the values obtained as a result of the work of diagnostic rules depending on the type of detector in the selected ML model branch.

If you need to hide the operating results from previously selected ML model branches, clear the check boxes next to these branches (however, one of the branches must remain active for graphs to be displayed in the **History** section).

3. If you need to display the MSE received as a result of data processing by a specific ML model branch:

   a. Click the settings button ⚙ below the tag graphs on the left side of the page.

   b. In the **MSE graph display settings** pane that appears on the right, select the branch from the **Model branch** drop-down list. You can select only one ML model branch from the list.

   c. Click the **Close** button.

   The MSE graph displays the MSE values for the selected branch of the ML model.

The lower part of the graph displays the dot indicators of incidents that were registered by the selected ML model branches. If the display of indicators for all tags is enabled, the dot indicators of incidents that were registered by all ML model branches will be displayed.

Selecting a date and time interval in the History section

Kaspersky MLAD lets you choose the date and a fixed time interval (scale) for displaying historical data or a user-defined time interval (for example, when an incident was detected).

To select the date for displaying historical data:

1. In the main menu, select the **History** section.

2. Click the calendar icon (📅) and select the date and time of the historical data to be displayed on the graphs.

3. Click the **Apply** button.

   The vertical blue line on graphs will indicate the selected date and time (in the center of the graph).

4. To select a new date and time (point) on the graph, click the location icon (📍) on the left of the time axis and select the relevant point on the time axis.

   The selected point will become the new center of the graph. The vertical blue dashed line will indicate the new date and time.

To select a time interval for displaying historical data:

1. In the main menu, select the **History** section.

2. On the opened page, do one of the following:

- If you need to display data for a fixed time interval, select the relevant time interval from the drop-down list. The following time intervals are available by default:

  - 1, 5, 10, 15, and 30 minutes
  - 1, 3, 6, and 12 hours
  - 1, 2, 15, and 30 days
  - 3 and 6 months
  - 1, 2, and 3 years

  If necessary, the system administrator can create, edit, or delete time intervals.

- If you need to display data for an arbitrary time interval, click the interval selection icon (⇄), which is located to the left of the time axis, select the required interval on the time axis and click on ✓. If you need to change the scale again, repeat this step.

The graphs of the defined preset will display the tag values for the selected time interval.

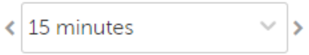
Navigating through time in the History section

Kaspersky MLAD provides the capability to navigate through time for convenient viewing of historical data.

To use time navigation when viewing data:

1. In the main menu, select the **History** section.
2. On the opened page, select the time interval for the data that you want to view.
3. Use the left (<) and right arrows (>) in the upper part of the page to move left or right along the time axis.

The time axis for viewing historical data on the graph will shift to the selected time interval.



Navigating through time

On graphs, a vertical blue dashed line indicates the midpoint of the selected time interval and matches the selected date and time. If an interval of **1 day** is selected, the graph displays historical data for the 12-hour periods before and after the selected date and time relative to the dashed line. If necessary, you can change the time interval.

Configuring how graphs are displayed in the History section

Kaspersky MLAD lets you configure the settings for displaying preset graphs in the **History** section.

To configure the display settings for preset graphs:

1. In the main menu, select the **History** section.

2. On the opened page, click the settings button ⚙ in the upper part of the screen.

   The **Graph display settings** pane will appear on the right.

3. In the **Graph height** drop-down list, select one of the following values: 55 px, 110 px, 145 px, 190 px.

   By default, the **Graph height** parameter is set to 55 px.

4. If necessary, use the **Show observation graphs in selected color** toggle switch to enable the display of tag observation graphs in a specific color, and select the color in the **Color of observation graphs** field.

5. If necessary, use the **Show prediction graphs in selected color** toggle switch to enable the display of tag prediction graphs in a specific color, and select the color in the **Color of prediction graphs** field.

6. If necessary, use the **Tag description and name** toggle switch to enable display of the tag description and name on graphs.

7. If necessary, turn on the **Predicted tag value** toggle switch to enable the display of the predicted tag value and values obtained as a result of the work of diagnostic rules on graphs.

8. If necessary, use the **Personal tag error** toggle switch to enable display of the personal tag error on graphs.

9. If necessary, use the **Display indicators for all incidents** toggle switch to enable display of the dot indicators for incidents registered by all ML model branches.

   If this mode is disabled, only the dot indicators for incidents that were registered by the selected ML model branches will be shown.

10. If you need the graphs to display the defined technical limits for a tag:

    a. Turn on the **Blocking threshold** toggle switch.

    b. If you need to always display the defined technical limits, turn on the **Always display blocking threshold** toggle switch.

       If this mode is disabled, the technical limits will be displayed only if the tag value has reached the corresponding limit in the graph area displayed on the screen.

11. If necessary, use the **Additional threshold lines** toggle switch to enable the display of additional threshold lines on the graph.

12. Click the **Close** button to return to viewing graphs in the **History** section.

The defined settings for displaying preset graphs in the **History** section will be applied.

Viewing data in the Time slice section

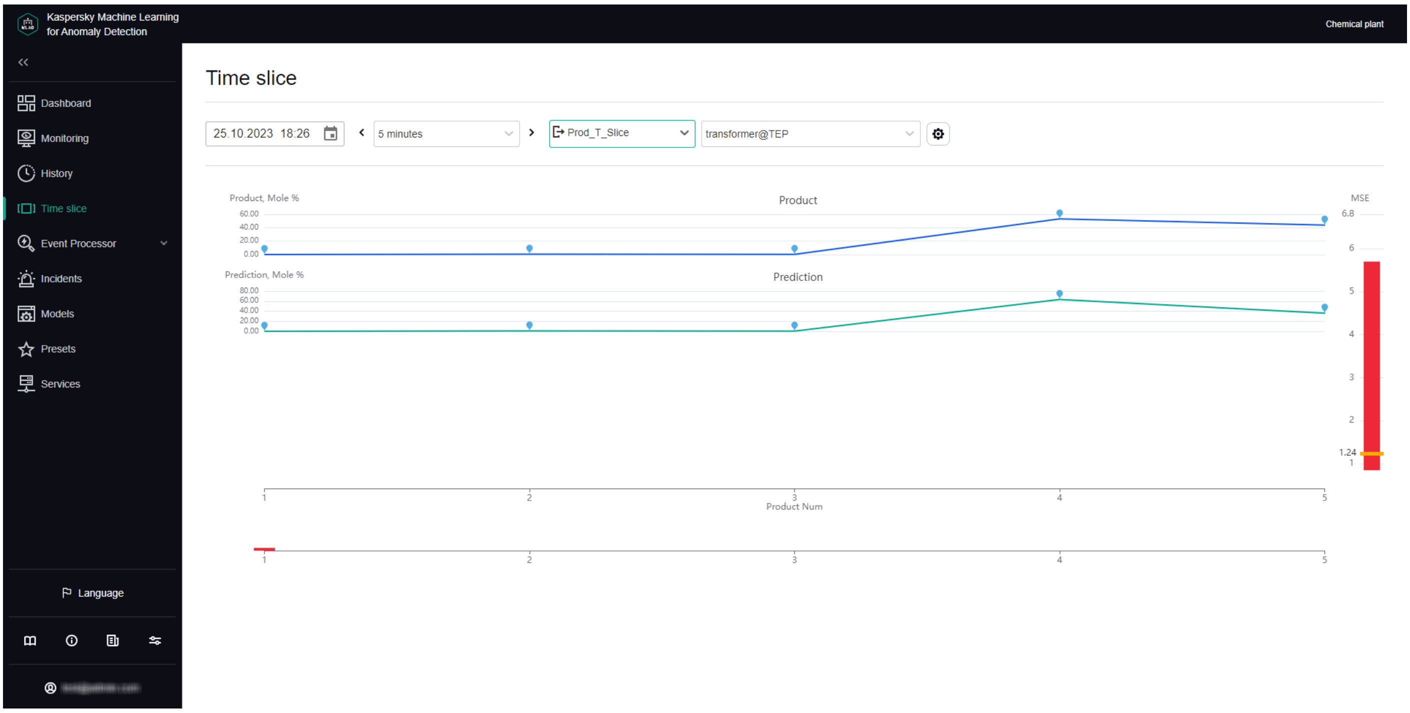
In the **Time slice** section, you can view the values of process parameters received from sensors of the monitored asset at the same point in time. The sensors must be of the same type (have the same dimension) and must be positioned linearly, like pressure sensors in an oil pipeline, for example.

Data is presented in the form of graphs that allow you to see whether an incident was detected at the selected time and where the likely source of the incident is located.

The lower part of the page contains a section displaying the individual errors of tags. The data is presented as a bar graph. The error value for each tag is displayed when the mouse cursor hovers over the relevant column. The MSE graph is located on the right of the preset tag graphs.

In the **Time slice** section, you can use the drop-down list to select a preset and the date and time when data was received. This list includes special presets that can be created in the **Presets** section. A special preset should contain only tags of the same type that have defined x-axis coordinates. You can additionally specify expressions dynamically calculated for each tag based on actual and predicted tag values, individual prediction errors, and tag coordinate values and constants defined in expressions.

You can also customize the display of graphs, select a time interval for viewing data, and select a specific element of the ML model to view the personal errors of preset tags obtained as a result of data processing by the selected element of the ML model.



Time slice section

Viewing data for a specific preset in the Time slice section

To view data for a specific preset:

1. In the main menu, select the **Time slice** section.
2. On the opened page, select the relevant preset from the **Preset** drop-down list.

   The page displays graphs for tags that are included in the selected preset.

If necessary, you can change the time interval for displaying data, customize the display of a graph, or select a specific branch of the ML model. You can also change which tags are displayed by editing the preset.

Selecting a specific branch of the ML model in the Time slice section

If the ML model used for a monitored asset has several branches for processing and predicting data, Kaspersky MLAD lets you select a specific branch of the ML model to display the personal tag errors obtained as a result of this branch in the **Time slice** section.

To view the personal tag errors resulting from data processing by a specific ML model branch:

1. In the main menu, select the **Time slice** section.
2. On the opened page, select the relevant branch of the ML model from the **Model branch** drop-down list.

   The name of the selected branch will be displayed in the field.

The tag graphs of the selected preset will display the personal tag errors resulting from data processing by the selected branch of the ML model.

Selecting a date and time interval in the Time slice section

Kaspersky MLAD lets you select a date and time interval (scale) for displaying incoming data.

To select the date for displaying incoming data:

1. In the main menu, select the **Time slice** section.
2. Click the calendar icon (📅) and select the date and time for displaying data on the graphs.
3. Click the **Apply** button.

   The graphs will display the tag values for the selected date and time.

To select a time interval for displaying incoming data:

1. In the main menu, select the **Time slice** section.
2. Select the required time interval from the drop-down list in the upper part of the opened page. The following time intervals are available by default:

   - 1, 5, 10, 15, and 30 minutes
   - 1, 3, 6, and 12 hours
   - 1, 2, 15, and 30 days
   - 3 and 6 months
   - 1, 2, and 3 years

   If necessary, the system administrator can create, edit, or delete time intervals.

The page will display graphs of the defined preset for the selected time interval.

Navigating through time in the Time slice section

Kaspersky MLAD provides the capability to navigate through time for convenient viewing of data.

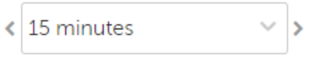
To use time navigation when viewing data:

1. In the main menu, select the **Time slice** section.

2. On the opened page, select the time interval for the data that you want to view.

3. Use the left (‹) and right arrows (›) in the upper part of the page to move left or right along the time axis.

The time axis for viewing data on the graph will shift to the selected time interval.



Navigating through time

Configuring how graphs are displayed in the Time slice section

Kaspersky MLAD lets you configure the settings for displaying preset graphs in the **Time slice** section.

To configure the display settings for preset graphs:

1. In the main menu, select the **Time slice** section.

2. On the opened page, click the settings button ⚙ in the upper part of the screen.

   The **Graph display settings** pane will appear on the right.

3. In the **Graph height** drop-down list, select one of the following values: 55 px, 110 px, 145 px, 190 px.

   By default, the **Graph height** parameter is set to 55 px.

4. Click the **Close** button to return to viewing the graphs.

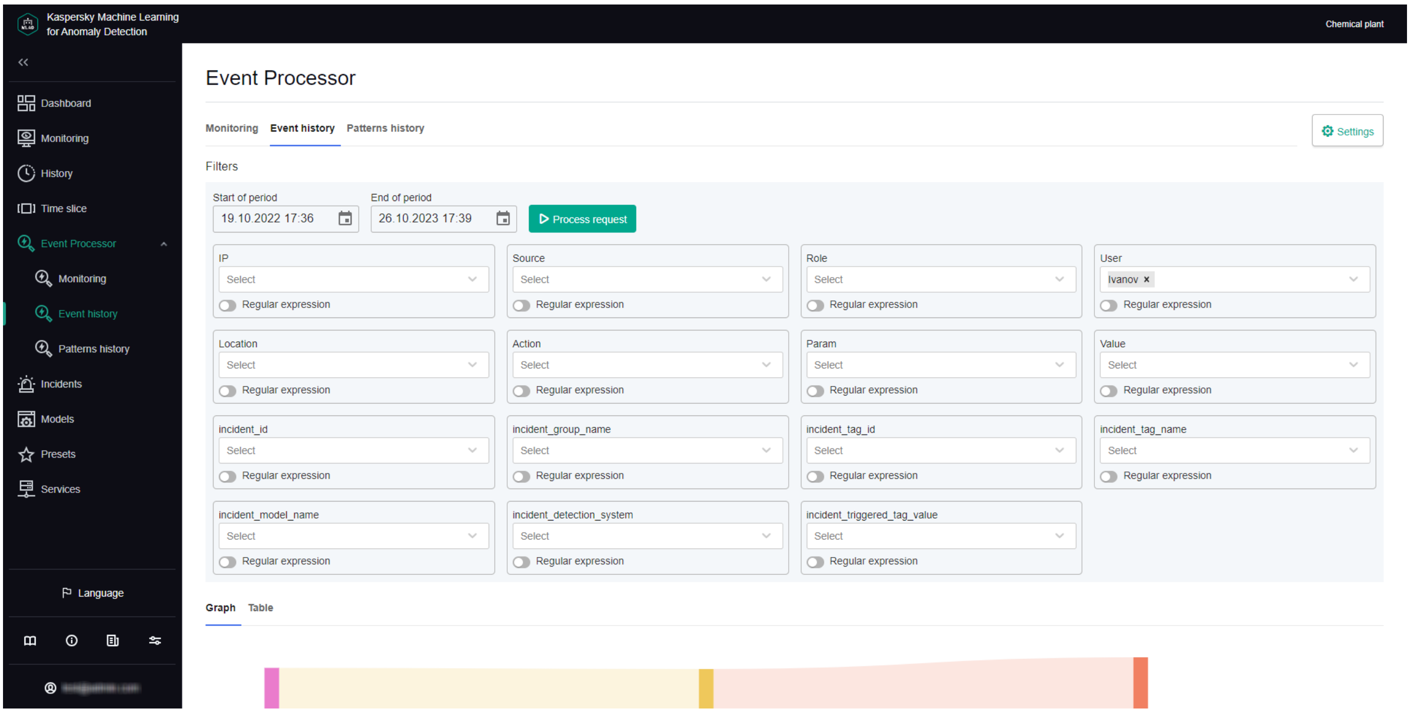
The configured graph display settings will be applied.

Working with events and patterns

The **Event Processor** section provides data on events and the structure of patterns detected by the Event Processor service in the event stream received from external sources or from the Anomaly Detector service.

In the **Event Processor** section, you can view the history of received events and the registration history of new and/or persistently recurring patterns. You can also configure the display of event parameters and can configure pattern registration settings. On the **Monitoring** tab, you can monitor specific events, patterns, or values of event parameters received by the Event Processor within the data stream from monitored assets.

If restarted, Kaspersky MLAD restores the state of the Event Processor service and pauses the processing of data received from the CEF Connector. This data is temporarily stored in the internal queue of the application message broker. Until the Event Processor service is restored, the **Event Processor** section tabs will display a notification informing you that the Event Processor service has stopped. This service restoration process may take several minutes if there is a significantly large number of processed events or registered patterns.



Start of period: 19.10.2022 17:36

End of period: 26.10.2023 17:39

User: Ivanov

Event Processor section

Configuring settings in the Event Processor section

Before events are processed by the Event Processor service, attention settings and display of event parameters must be configured.

System administrators can manage the attention settings and display of event parameters.

A large number of attention directions can slow down the operation of Kaspersky MLAD main services (data reception, anomaly detection, web interface). To clarify the number of attention directions, it is recommended to consult with Kaspersky experts or a certified integrator.

To configure attention settings and display of event parameters:

1. In the main menu, select the **Event Processor** → **Monitoring** section.

2. On the opened page, click the **Settings** button.

   The **Event Processor settings** pane will appear on the right.

3. In the **Configure attention** section, do one of the following for each event parameter:

   - If you need to register patterns for all values of an event parameter, use the drop-down list to select **All parameter values**.

   - To register patterns for a specific event parameter value, select the event parameter value in the drop-down list. As you start typing a value, all matching parameter values are displayed in the list.

     If the parameter value is not listed, enter the required value and select **Create Value: <event parameter value>**.

- If you need to register patterns based on an event parameter value template, turn on the **Regular expression** toggle switch for the relevant event parameter, use the drop-down list to enter the value template with a regular expression, and select **Regular expression: <value template>**.

  You can use special characters of regular expressions to search for patterns based on regular expressions.

Each attention direction is defined by the parameter value that must be present in all events of this direction. When configuring attention directions, you can indicate specific values or templates of values of one or more parameters or define attention directions for all possible values of one or more parameters.

4. To configure the display of filters for the event parameters, in the **Filters** section on the **Event history** and **Patterns history** tabs, in the **Configure display of event parameter filters** section, select the check boxes next to the names of the desired event parameters.

   By default, the **Configure display of event parameter filters** section displays the **event parameters from the Anomaly Detector service**. To display custom event parameters, load the Event Processor service configuration file. All available event parameters are selected by default.

   > If the **Process incidents as events** function is enabled, the Event Processor receives events with the following parameters:
   >
   > - **incident_detection_system** – the name of the detector that registered the incident.
   > - **incident_model_name** – the name of the ML model used.
   > - **incident_tag_name** – the name of the tag whose behavior invoked registration of the incident.
   > - **incident_group_name** – the name of the incident group to which the registered incident belongs.
   > - **incident_triggered_tag_value** – the value of the tag whose behavior invoked registration of the incident.
   > - **incident_id** – the ID of the registered incident.
   > - **incident_tag_id** – the ID of the tag whose behavior invoked registration of the incident.

   If necessary, in the **Filters** section you can change the display order for the event parameters. For this purpose, drag the required event parameter up or down in the **Configure display of event parameter filters** section.

5. To save your changes, click the **Apply** button.

Working with monitors

> Monitor management is available to system administrators.

In the **Event Processor** → **Monitoring** section, you can create monitors for monitoring specific events, patterns, or values of event parameters.

The **Monitoring** tab displays all monitors created in the application, including the following brief information:

- Monitor name.
- **Monitor threshold**.

> When this number of monitor activations (threshold) on the sliding window is reached, the application sends an alert about monitor activation to the external system.

- Sliding window used to track the number of monitor activations.
- Number of monitor activations on the sliding window.

If necessary, you can view detailed information about each monitor by clicking the **Information** button located next to the name of the relevant monitor in the table.

- **Monitor ID** is the unique identifier of the monitor being viewed.
- **Number of activations on the sliding window** refers to the number of registered monitor activations on the sliding window.
- **Date and time of last activation** refers to the date and time when the monitor was last activated.
- **Activated** refers to the type of element that caused the monitor activation. Monitor activation may be invoked by a new or existing event parameter value, event, pattern, or another monitor.
- **Subscription** indicates what is being tracked by the viewed monitor: event parameter values, events, or patterns.
- **Sliding window** indicates the time interval from the current time back to the time sequence for which the number of activations is taken into account. This window shifts synchronously with the passage of time according to the timestamps in events.
- **Threshold** indicates the number of activations to be registered by the monitor on the sliding window before sending an alert about the monitor activation to the external system via the CEF Connector.
- **Filters** is a table containing information about filters for event parameters observed by the current monitor to track event parameter values, events, and patterns. The following data is displayed for each element:
  - **Parameter name** refers to the names of event parameters whose values are being observed by the viewed monitor.
    Each monitored asset has its own specific incoming events and event parameters. The names of event parameters are defined in the configuration file for the Event Processor service. The configuration file is created and uploaded by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator during configuration of the Event Processor service.
  - **Type** defines which types of values are being tracked by the monitor: specific values, new values, or all values.
  - **Purpose** defines which event parameters are receiving focused attention from the model.
  - **Values** refers to the values of event parameters that are being observed by the viewed monitor.
- **Stack limit** determines the number of most recent monitor activations displayed in the **Activation stack** table.
- **Activation stack** is a table that contains information about the latest activations of the monitor:
  - **Parameter value ID** is the ID of the event parameter value whose detection caused the monitor activation. This parameter is displayed only when the monitor is activated by an event parameter value.
  - **Event ID** is the ID of the event whose detection caused the monitor activation. This parameter is displayed only when the monitor is activated by an event.
  - **Pattern ID** is the ID of the pattern whose detection caused the monitor activation. This parameter is displayed only when the monitor is activated by a pattern.
  - **System parameters** is a group of system settings containing the following information:
    - **Event time** is the date and time when the event is detected in the event stream.

        - **Interval from previous item** is the time interval between the current and the previous event in the event stream on the sliding window. Kaspersky MLAD displays the time intervals between events upon the first detection of the pattern containing the events. When a pattern is detected again, the Event Processor takes into account the coefficient of allowed intervals dispersion specified by the administrator for these events.

        - **Total activations** is the number of event occurrences in the event stream on the sliding window.

        - **Parameter count** is the number of event parameters for which the values were received from the monitored asset.

        - **Last activation** is the date and time when the event was last detected in the event stream on the sliding window.

    This group of parameters is displayed only when the monitor is activated by an event or an event parameter value.

    - **Activation date and time** is the date and time when the monitor was activated. This parameter is displayed only when the monitor is activated by a pattern.

    - **Event parameter** is the value of the event parameter received from the monitored asset. This parameter is displayed only when the monitor is activated by an event parameter value.

    - **Event parameters** are the values of the parameters of the event received from the monitored asset. This parameter is displayed only when the monitor is activated by an event.

    - **Events** is the number of events included in the pattern that caused the monitor activation. This parameter is displayed only when the monitor is activated by a pattern.

    You can view information about the events included in the pattern by clicking the number of events in the corresponding row of the table. Clicking the number of events displays information about IDs, system settings, and parameters of the event included in the selected pattern.

On the **Histogram** tab, you can also view brief statistics on the number of registered activations for each created monitor.

Creating a monitor

Monitor management is available to system administrators.

To create a monitor:

1. In the main menu, select the **Event Processor** → **Monitoring** section.

2. Click the **Create monitor** button.

   The **Create monitor** pane appears on the right.

3. Specify the monitor name in the **Name** field.

4. In the **Sliding window (sec.)** field, specify the interval (in seconds) from the current point in time back to the time sequence for which the monitor will process incoming values of parameters, events or patterns.

5. In the **Threshold** field, specify the number of monitor activations in the sliding window after which the monitor sends an alert to the external system.

6. In the **Stack limit** field, specify the number of monitor activations that must be displayed when viewing information about the monitor.

7. In the **Subscription type** drop-down list, select one of the following values:

   - If you need to process data on the values of event parameters, select **Parameter values**.

   - If you need to process data on events, select **Events**.

   - If you need to process data on detected patterns, select **Patterns**.

8. If you need to track new events, patterns, or values of event parameters, turn on the **Only new** toggle switch in the **Filters** section.

9. To focus the attention of the model on specific directions of events, do one of the following:

   - If you selected **Events** from the **Subscription type** drop-down list, select **Attention** for the relevant event parameter. If you need to track events without specifying the attention direction, clear the **Attention** check box.

   - If you selected **Patterns** from the **Subscription type** drop-down list, select the **Attention** check box for the relevant event parameter.

   You can select only one attention direction.

10. For each event parameter, do one of the following:

    - If you need to process data on all values of an event parameter, use the drop-down list to select **All parameter values**.

      This option is displayed if you specified the attention direction for the current event parameter.

    - To process data only on the new values of an event parameter, in the drop-down list select **New parameter values**.

      This option is displayed only when the **Only new** function is enabled for event-based data processing.

    - To process data for a specific value of an event parameter, in the drop-down list select the event parameter value. As you start typing a value, all matching parameter values are displayed in the list.

      If the parameter value is not listed, enter the required value and select **Create Value: <event parameter value>**.

    - If you need to process data based on an event parameter value template, turn on the **Regular expression** toggle switch for the relevant event parameter, use the drop-down list to enter the value template with a regular expression, and select **Regular expression: <value template>**.

      You can use special characters of regular expressions to search patterns using regular expressions.

11. Click the **Create** button.

The new monitor is created and displayed on the **Monitoring** tab.

Deleting a monitor

Monitor management is available to system administrators.

To delete a monitor:

1. In the main menu, select the **Event Processor** → **Monitoring** section.
2. Click the **Delete** button in the cell of the monitor whose information you want to delete and confirm your selection.

   The monitor will be deleted.

Viewing the events history

Kaspersky MLAD lets you view the events that were received from external sources of events. To view events, you need to upload them to **Event Processor** → **Event history**.

Viewing the event history is available to system administrators.

Kaspersky MLAD displays incoming events as a graph of relations between event parameters. The graph nodes correspond to the values of the event parameters, and the arcs between the nodes correspond to the links between the parameter values of incoming events. You can hover the mouse pointer over the event graph and view information about the event parameters and their values. You can also hover the mouse pointer over the event graph arc and view information about the number of links between the values of event parameters.

You can also view **information about the detected events** as a table.

- **Event ID** is the ID of the detected event.
- **System parameters** contain the following information about the event:
  - **Last detection in interval** is the date and time when the event was last detected in the event stream during the specified period.
  - **Detections count in interval** is the number of event detections in the event stream during the specified period.
  - **Parameter count** is the number of event parameters for which the values were received from the monitored asset.
  - **Last activation** is the date and time when the event was last detected in the event stream.
- **Event parameters** are the values of the event parameters received from the monitored asset.

Each monitored asset has its own specific incoming events and event parameters. The list of event parameters is defined in the configuration file for the Event Processor service. The configuration file is created and uploaded by a system administrator during configuration of the Event Processor service.

To upload data for viewing incoming events:

1. In the main menu, select the **Event Processor** → **Event history** section.

2. In the **Filters** section, click the calendar icon (📅) to select the start and end date and time of the period for which you want to load and view events. To configure event parameters, do one of the following:

   - To load events based on the specific values of the event parameters, select the event parameter value in the drop-down lists. As you start typing a value, all matching parameter values are displayed in the lists.

   - To load events based on a value template, enable the **Regular expression** option for the relevant event parameters, in the drop-down lists, specify the value template using a regular expression, and select **Regular expression: <value template>**.

     You can use special characters of regular expressions to perform a search based on regular expressions.

   Each monitored asset has its own specific set and names of event parameters.

3. Click the **Process request** button.

   Data on the events found by the application will be displayed as a graph in the central part of the page.

4. To view the received events as a table, select the **Table** tab.

   The central part of the page displays a table that contains information on the detected events.

Viewing the pattern history

In the section **Event Processor** → **Patterns history**, you can find and view the structure of the new and/or persistently recurring patterns. The Event Processor generates patterns only for specific directions that are defined in the attention configuration by the system administrator.

Viewing the pattern history is available to system administrators.

You can also view the structure of the detected patterns down to the event level. The Event Processor represents patterns, events, and values of event parameters as a layered hierarchy of nested elements. For example, a fourth-layer pattern consists of subpatterns of the third layer. A third-layer pattern consists of second-layer patterns, and a second-layer pattern consists of events, which are first-layer elements. Event parameter values are elements of the null terminal layer.

Each monitored asset has its own specific incoming events and event parameters. The list of event parameters is defined in the configuration file for the Event Processor service. The configuration file is created and uploaded by a system administrator during configuration of the Event Processor service.

To view the registered patterns:

1. In the main menu, select the **Event Processor** → **Patterns history** section.

2. In the **Filters** section, configure the following settings for displaying patterns on the page:

   a. In the **Start of period** field, click the calendar icon (📅) and select the starting date and time of the period for which you want to view the patterns.

   b. In the **End of period** field, click the calendar icon (📅) and select the end date and time of the period for which you want to view the patterns.

c. In the **Pattern type** drop-down list, select one of the following values:

   - **Stable** refers to patterns that were registered by the Event Processor service two or more times.
   - **New** refers to new patterns registered by the Event Processor service for the first time.
   - **All** includes all patterns that were registered by the Event Processor service.

d. To view patterns for a specific attention direction, select **Attention** for the relevant event parameter.

   You must select one of the attention directions that were defined when configuring the attention settings.

e. To configure event parameters, do one of the following:

   - To view patterns based on specific values of the event parameters, select the event parameter values in the drop-down lists. As you start typing a value, all matching parameter values are displayed in the lists.
   - If you need to view patterns based on a value template, turn on the **Regular expression** toggle switch for the relevant event parameters, use the drop-down lists to enter the value template with a regular expression, and select **Regular expression: <value template>**.

     You can use special characters of regular expressions to perform a search based on regular expressions.

   For the request to be processed correctly, enter the values for the event parameter that is receiving focused attention from the model. If an event parameter that is receiving focused attention has multiple values defined, the Event Processor will generate patterns for each value of the parameter.

3. Click the **Process request** button.

   The central part of the page displays a table containing **data on the registered patterns**.

   - **Pattern ID** is the ID of the pattern. The first digit of the pattern ID corresponds to the number of the layer where this pattern was detected.
   - **Last detection in interval** is the date and time when the pattern was last detected in the event stream of the monitored asset during the specified period.
   - **Detections count in interval** is the number of pattern detections in the event stream of the monitored asset during the specified period.
   - **Event count** is the number of events in the pattern.
   - **Last activation** is the date and time when the pattern was last detected in the event stream of the monitored asset or in the sleep mode.

4. To view the pattern structure, click the desired pattern row.

   The page with **detailed information on the pattern** opens.

- **Pattern ID** is the ID of the selected pattern. The first digit of the pattern ID corresponds to the number of the layer where this pattern was detected.
- **Event count** is the number of events in the pattern.
- **Interval from previous item** is the time interval between the selected pattern and the pattern detected in the pattern sequence on the current layer before the selected pattern. Kaspersky MLAD displays the time intervals between the elements of the selected pattern when it is first detected. When a pattern is detected again, the Event Processor takes into account the coefficient of allowed intervals dispersion specified by the administrator for the elements of this pattern.
- **Total activations** is the number of detections of the selected pattern in the event stream for the specified period.
- **Pattern end time** is the end date and time of the selected pattern in the sequence of patterns on the current layer.
- **Last activation** is the date and time when the pattern was last detected in the event stream or in the sleep mode.
- **Patterns** is a tab that displays a table with information about the patterns included in the selected pattern. The following information is displayed on the **Patterns** tab:
    - **<layer number> layer** is a set of tabs for viewing information on the patterns included in the selected pattern on different layers of its structure. The tabs are displayed if you select a pattern detected on the fourth layer or higher. You can view patterns up to the second nesting level.
    - **Pattern ID** is the ID of the subpattern. The first digit of the pattern ID corresponds to the number of the layer where this pattern was detected.
    - **Pattern end time** is the end date and time of the subpattern in the sequence of patterns on the selected layer.
    - **Total activations** is the number of detections of the subpattern in the structure of the selected pattern.
    - **Event count** is the number of events in the subpattern.
    - **Interval from previous item** is the time interval between the subpattern and the previous pattern in the table. Kaspersky MLAD displays the time intervals between the elements of the subpattern when it is first detected. When a pattern is detected again, the Event Processor takes into account the coefficient of allowed intervals dispersion specified by the administrator for the elements of this pattern.
    - **Last activation** is the date and time when the subpattern was last detected in the sequence of patterns on the selected layer or in the sleep mode.
- **Events** is a tab that displays a table of events included in the selected pattern. The following data is displayed for each event:
    - **Event ID** is the ID of the event.
    - **System parameters** contain the following information about the event:
        - **Event time** is the date and time when the event is detected in the pattern structure.

        - **Interval from previous item** is the time interval between the current event and the previous event in the table. Kaspersky MLAD displays the time intervals between the events of the selected pattern when it is first detected. When a pattern is detected again, the Event Processor takes into account the coefficient of allowed intervals dispersion specified by the administrator for the events of this pattern.

        - **Total activations** is the number of the event repeated occurrences in the structure of the selected pattern during the specified period.

        - **Parameter count** is the number of event parameters for which the values were received from the monitored asset.

        - **Last activation** is the date and time when the event was last detected in the event stream.

    - **Event parameters** are the values of the parameters of the event received from the monitored asset.

5. To view the structure of a pattern, do one of the following:

    - To view the structure of a particular subpattern, on the **Patterns** tab in the **Nested elements** section, click the desired pattern.

      You can return to viewing the top-level pattern structure by clicking the ID of the desired pattern above the **Pattern info** section.

    - To view the table of subpatterns at a certain nesting level, select the desired layer on the **Patterns** tab of the **Nested elements** section.

    - To view the events included in the pattern at the current nesting level, click the **Events** tab.

   Kaspersky MLAD displays the pattern structure from the top nesting level.

Working with incidents and groups of incidents

In Kaspersky MLAD, an ML model can simultaneously use multiple types of detectors that analyze incoming telemetry data and detect incidents independent of each other. The Kaspersky MLAD web interface provides the capability to investigate detected incidents. Depending on the type of detector that registered an incident, information about the incident and the methods you can use to investigate it may differ.

You can perform the following actions for any incident:

- Analyze the incident details.

- Find out if any similar incidents were detected previously.

- Study the behavior of the monitored asset at the moment when the incident was detected.

- Leave a note or expert opinion for a registered incident or incident group.

The **Incidents** section displays a column graph showing the incidents that match the filtering criteria specified under the graph. The graph displays statistics on the registered incidents for the period specified above the graph.

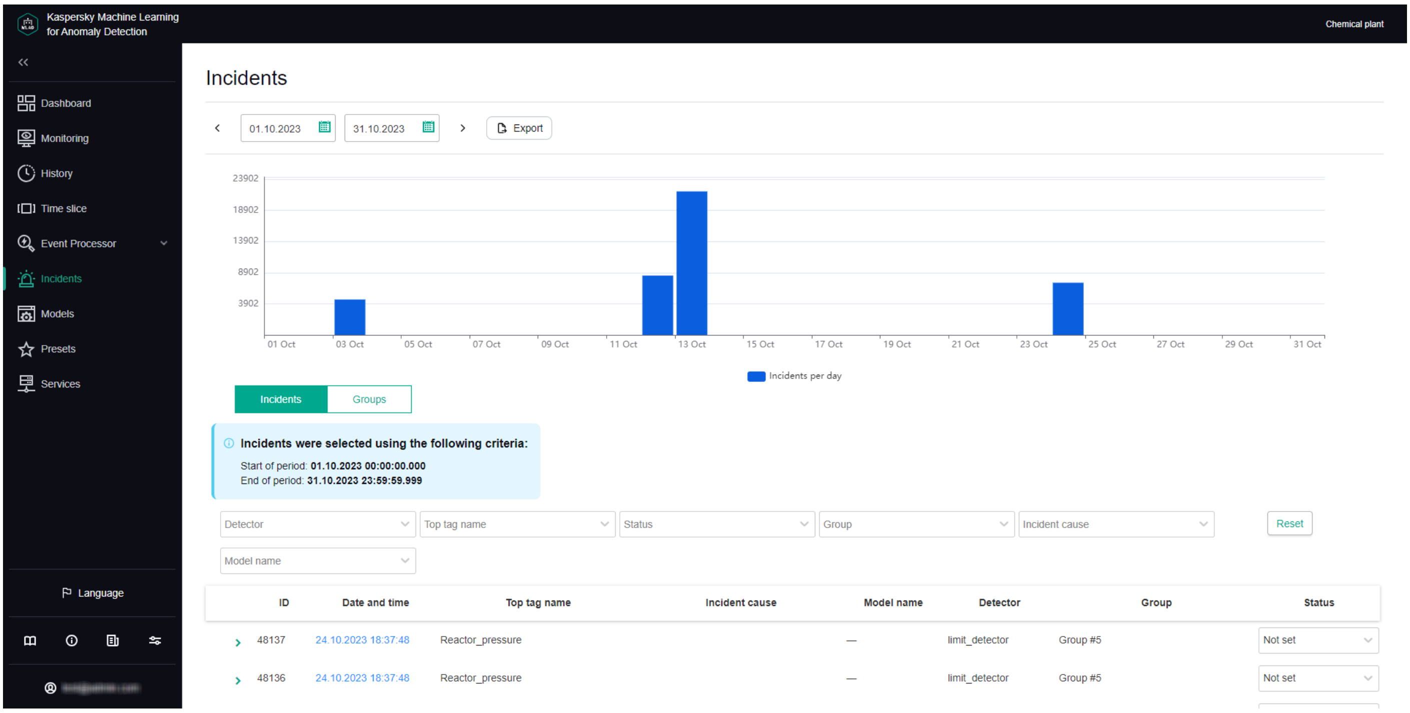
The graph can display up to 60 bars. If the specified period does not exceed 60 days, incidents on the graph are grouped by days. If the specified period is between 60 days and 60 weeks, incidents on the graph are grouped by weeks. If the specified period is longer than 60 weeks, incidents on the graph are grouped by months.

Hovering the mouse pointer over a bar of the graph displays a window showing the number of registered incidents per corresponding time period. Upon clicking a bar, the graph and in the table below display information about the incidents registered during the corresponding time period.

In this section, you can view individual incidents as well as groups of incidents.

Incidents tab

The **Incidents** tab shows a table of registered incidents. Incidents are sorted by date in descending order, with the newest incidents shown first.



Incidents were selected using the following criteria:

Start of period: **01.10.2023 00:00:00.000**
End of period: **31.10.2023 23:59:59.999**

	ID	Date and time	Top tag name	Incident cause	Model name	Detector	Group	Status
›	48137	24.10.2023 18:37:48	Reactor_pressure		—	limit_detector	Group #5	Not set
›	48136	24.10.2023 18:37:48	Reactor_pressure		—	limit_detector	Group #5	Not set

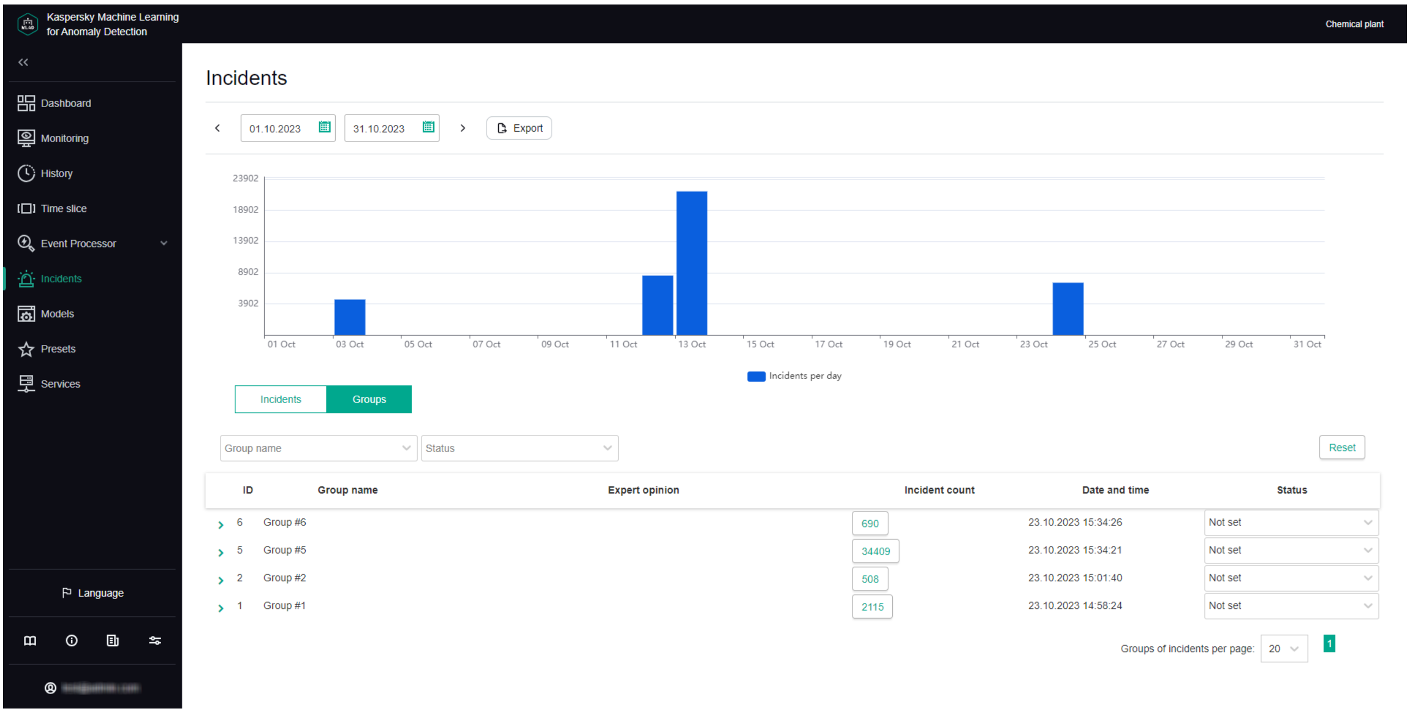
Incidents tab

You can go to the **History** section by clicking the date and time of the incident.

Groups tab

The **Groups** tab shows a table of incident groups. Kaspersky MLAD automatically generates groups of similar incidents.

You can change the group name that was assigned automatically and set the status of incidents that belong to this group. You can also provide an expert opinion that contains the recommended actions to take in response to new incidents in this group, for example.



ID	Group name	Expert opinion	Incident count	Date and time	Status
6	Group #6		690	23.10.2023 15:34:26	Not set
5	Group #5		34409	23.10.2023 15:34:21	Not set
2	Group #2		508	23.10.2023 15:01:40	Not set
1	Group #1		2115	23.10.2023 14:58:24	Not set

Groups tab

Scenario: analysis of incidents

This section describes the sequence of actions required when analyzing incidents registered by Kaspersky MLAD.

> The incident analysis scenario described in this section is not a precisely regulated procedure. The specific scope and sequence of actions taken to investigate an incident and identify its cause depend on the particular subject area, the knowledge level of the process engineer or ICS expert investigating the incident, and the availability of additional information on the monitored asset.

The incident analysis scenario consists of the following steps:

1. **Viewing information about a registered incident**

   The Incidents section displays all incidents registered by Kaspersky MLAD, and provides detailed information about their registration time, the detector that registered the incident, and an expert opinion if one was added. You can proceed to view incident information in one of the following ways:

   - **Viewing the latest incidents in the Dashboard section**

     If you want to view a recently detected incident, in the Dashboard section, click the date and time of the relevant incident in the **Latest incidents** table. In the History section that opens, in the lower part of the page, click the dot indicator in the *MSE* section to view a specific incident. The Incidents section opens showing only the incidents that were registered in the specific time interval represented by the selected dot indicator (the interval is displayed above the incidents table).

   - **Viewing incidents in the Incidents section**

     If you know the date and time when an incident was registered, select the corresponding incident in the Incidents section. You can change the time interval for the displayed incidents by using the bar graph or the date selection field in the upper part of the page.

   - **Navigating from an incident notification received by email**

If an incident notification was created for you, you will receive the notification by email when an incident is registered. The email message contains the time when the incident began, the most anomalous tag, and a link to proceed to the **History** section in the Kaspersky MLAD web interface. You can use this link to proceed to the start of the incident in the **History** section. At the bottom of the **History** page, click on the dot indicator in the MSE section according to the incident start time. The **Incidents** section opens showing only the incidents that were registered in the specific time interval represented by the selected dot indicator (the interval is displayed above the incidents table).

When you find a record about the required incident, click the right arrow (›) to view detailed information about the incident.

2. **Viewing information about similar incidents**

   When two or more similar incidents are detected, Kaspersky MLAD automatically combines them into a group. In the incidents table in the **Incidents** section, the group associated with the incident is displayed in the **Group** column. If nothing is indicated for the selected incident in this column, this means that Kaspersky MLAD has not yet detected incidents similar to this particular incident.

   To view all incidents in a group, select the **Groups** tab and click the right arrow (›) next to the relevant group. The table displays information about the incidents assigned to the selected group, as well as an expert opinion if it was added. Read the expert opinions for individual incidents and for the group.

3. **Studying the behavior of the monitored asset at the moment when an incident was detected**

   Study the behavior of the monitored asset at the moment when the incident was detected.

4. **Analyzing the incident**

   Analyze the incident while considering the specific details of incident registration depending on the type of detector that registered the incident:

   - **Forecaster**. The neural network element of the ML model registers incidents when deviations in the behavior of the monitored asset are detected. Based on information obtained when viewing the automatically generated Tags for event #N preset and considering the available expert knowledge on the monitored asset, form a hypothesis regarding which tags could have caused the incident and select the appropriate preset after studying their behavior. Analyze the MSE graph, move back in time from the moment the MSE threshold was reached, and examine the behavior of tags at the moment when the MSE values started to grow.

   - **Rule Detector**. For each incident registered by elements of the ML model on the basis of a diagnostic rule, the Tags for event #N preset is automatically generated, which includes the value obtained as a result of the diagnostic rule operation and which caused the incident registration.

   - **Limit Detector**. For each incident that was registered by the Limit Detector, the application automatically creates the Tags for event #N preset, which includes a single causal tag for the incident.

   - **Stream Processor**. The Stream Processor service registers incidents up until telemetry data is transmitted to the ML model for processing. Incidents are registered if data loss is detected or if observations are received by Kaspersky MLAD too early or too late.

5. **Adding a status, cause, expert opinion or note to an incident or its incident group**

   For each incident, add an expert opinion or note in which you can specify whether the incident is an anomaly. An expert opinion and note for an incident are displayed only when viewing a specific incident. If necessary, you can specify the status and cause of an incident. The cause of an incident is displayed in the incidents table and when viewing a specific incident. You can also add or edit the status and expert opinion for a group of incidents.

Viewing incidents

To view incidents that were registered on a specific date:

1. In the main menu, select the **Incidents** section.

2. In the upper part of the opened page, on the bar graph, click the graph column for the relevant date.

3. If necessary, filter incidents by detector, top tag, status, group, or incident cause by selecting relevant values in the corresponding drop-down list.

   The table located in the central area of the page shows the incidents registered on that day according to the specified filtering criteria. When you click the **Reset** button, the table and the bar graph show all registered incidents.

The following information is displayed for each incident in the table:

- **ID** refers to the ID of the registered incident.

- **Date and time** refers to the date and time when the incident was registered.

  Clicking the incident registration date opens the **History** section, where you can view information about the "Tags for event #N" preset generated for the registered incident.

- **Top tag name** refers to the name of the process parameter for which the largest deviation from the prediction was recorded at the time of incident registration.

- **Incident cause** refers to the cause of a logged incident added by the expert (process engineer or ICS specialist) after incident analysis or defined by the ML model.

- **Model name** refers to the name of the ML model whose element registered the incident.

- **Detector** refers to the name of the detector that identified an anomaly and registered the incident: Forecaster, Limit Detector, Rule Detector, Stream Processor.

- **Group** refers to the name of the incident group to which the registered incident belongs.

  If two or more similar incidents are detected, they are combined into a group that is created automatically by using the Similar Anomaly service. You can view only those incidents included in the group by selecting the group name from the drop-down list.

- **Status** refers to the status of a logged incident specified by the expert (process engineer or ICS specialist) after incident analysis or defined by the ML model.

  You can set the incident status based on analysis results by selecting the appropriate value from the drop-down list. After installation of Kaspersky MLAD, the following statuses of incidents and incident groups are available by default: **Under review**, **Decision pending**, **Instructions issued**, **Problem closed**, **Cause unknown**, **Ignore** and **False positive**. If necessary, the system administrator can create, edit, or delete statuses of incidents.

Viewing the technical specifications of a registered incident

In the **Incidents** section, you can view the technical specifications of registered incidents. To do so, click the right arrow (›) next to the relevant incident in the incidents table. The following technical specifications will be displayed for the selected incident:

- **Incident** is the section containing **information about the incident** ?.

  - **Model name** refers to the name of the utilized ML model.
  - **Model branch** is the name of the ML model branch. This is absent if the ML model has no branches.
  - **Detector** refers to the name of the detector that identified an anomaly and registered the incident: Forecaster, Limit Detector, Rule Detector, Stream Processor.
  - **MSE value** is the value of the individual mean square error.
  - **Threshold value** refers to the MSE threshold value for the ML model branch in use at the time of incident registration.

- **Top tag** is the section containing **information about the tag** for which the incident was registered.
  - **Top tag name (top tag ID)** is the name and ID of the tag whose behavior invoked registration of the incident.

    If an incident was registered by the Forecaster Detector, the name of the most anomalous tag that influenced the registration of the incident more than the other tags will be displayed. For the Rule Detector, the value of this parameter shows a value obtained as a result of the work of the diagnostic rule. For the Limit Detector, the tag whose value exceeded the blocking threshold defined for this tag will be displayed.
  - **Top tag value** is the value of the top tag registered when the incident occurred.
  - **Blocking threshold** refer to the thresholds of the top tag values, upon reaching which it is necessary for the ICS to take emergency response measures.
  - **Description** refers to a description of the top tag.
  - **Measurement units** refer to the units for measuring the top tag values.

- **Stream Processor service incident parameters** is a section containing **information about the parameters of the incident registered by the Stream Processor service**. This group of parameters is displayed if the current incident is registered by the Stream Processor service.
  - **Incident type** is the type of incident registered by the Stream Processor service. The Stream Processor service registers incidents when it detects observations that were received by Kaspersky MLAD too early or too late, or if the incoming data stream from a certain tag is terminated or interrupted.
  - **Data date and time** is the date and time when the observation was generated according to the monitored asset time. This parameter is displayed only for the **Late receipt of observation** and **Clock malfunction** incident types.
  - **Lag / Lead** is the amount of time by which the observation generation time lags behind or is ahead of the time the observation was received in Kaspersky MLAD. If data is received too early, the parameter value is displayed with a plus sign (+). If data is received too late, the parameter value is displayed with a minus sign (-). This parameter is displayed only for the **Late receipt of observation** and **Clock malfunction** incident types.

- **Incident cause** is the field for selecting the cause of the incident. This field is completed by an expert (process engineer or ICS specialist). If necessary, the system administrator can create, edit, or delete causes of incidents.

- **Expert opinion** is the field for adding an expert opinion based on an analysis of the registered incident. This field is completed by an expert (process engineer or ICS specialist).

- **Note** is the field for entering a comment for the selected incident. If necessary, you can provide a comment for the incident.

Viewing incident groups

When two or more similar incidents are detected, Kaspersky MLAD automatically combines them into a group (using the Similar Anomaly service). This lets you analyze incidents with consideration of prior history and expert opinions that were generated for similar incidents. In the incidents table in the **Incidents** section, the group associated with the incident is displayed in the **Group** column. If nothing is indicated for the incident in this column, this means that Kaspersky MLAD has not yet detected incidents similar to this particular incident. Incidents can be regrouped, and the expert opinions that were added to these incidents are migrated to the new group. The group name is automatically assigned in the format Group #N (N is replaced by the sequence number of the group). If necessary, you can edit a group name.

To view incident groups:

In the main menu, select the **Incidents** section and click **Groups**.

All incident groups for your monitored asset are displayed in the table located in the central part of the page.

The following information is displayed for each incident group in the table:

- **ID** is the incident group identifier.

- **Group name** refers to the name of the incident group.

- **Expert opinion** is a conclusion added by an expert (process engineer or ICS specialist) based on an analysis of the group of registered incidents.

- **Incident count** refers to the number of registered incidents included in the group.

  You can proceed to view incidents of the group by clicking **Incident count**.

- **Date and time** refers to the date and time when the incident group was created.

- **Status** refers to the status of registered incidents in a group specified by an expert (process engineer or ICS specialist) based on the results of the incident analysis.

  You can set the incident group status based on analysis results by selecting the appropriate value from the drop-down list. After installation of Kaspersky MLAD, the following statuses of incidents and incident groups are available by default: **Under review**, **Decision pending**, **Instructions issued**, **Problem closed**, **Cause unknown**, **Ignore** and **False positive**. If necessary, the system administrator can create, edit, or delete statuses of incidents.

To view detailed information about an incident group:

1. Click the right arrow (›) next to the incident group.

   A list of incidents in this group is displayed. The following technical specifications are displayed for each incident of the group:

   - **Incident date** is the date and time when the incident was registered.

     You can go to the **History** section by clicking the incident registration date.

- **Top tag name** is the name of the process parameter that had the largest impact when the incident occurred.
- **Top tag value** is the registered value of the tag that had the largest impact when the incident occurred.
- **Relevant tags** refers to a table that contains the identifiers of tags that influenced the identification of similar incidents and merging of these incidents into a group.

2. If you need to view the degree of influence a tag had on the formation of similar incidents, click the **Relevant tags** table cell containing the identifier of the relevant tag.

   All table cells containing the selected tag ID are highlighted in green. The closer the green-highlighted cells containing the ID of the selected tag are to the first table column, the more impact that tag has when identifying and grouping similar incidents.

You can also add a status and expert opinion for the incident group.

Studying the behavior of the monitored asset at the moment when an incident was detected

This section describes the sequence of actions required when studying the behavior of a monitored asset at the moment when an incident was detected.

Studying the behavior of a monitored asset consists of the following steps:

1. **Viewing the history of tags received for a monitored asset in the History section**

   You can proceed to view incident information in one of the following ways:

   - If you want to view a recently detected incident, in the **Dashboard** section, click the date and time of the relevant incident in the **Latest incidents** table.
   - In the **Incidents** section, click the date and time of the relevant incident in the incidents table.
   - If an incident notification was created for you, you can proceed to view the incident by clicking the link from the email notification. The email message contains the time when the incident began, the most anomalous tag, and a link to proceed to the **History** section in the Kaspersky MLAD web interface.

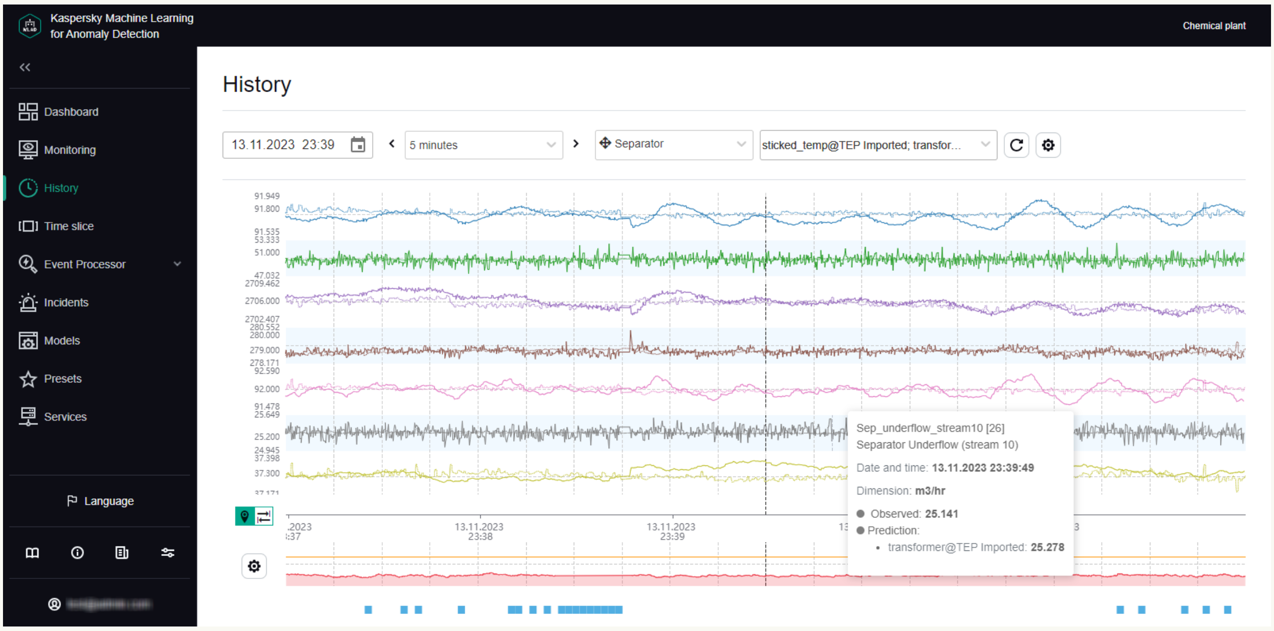
   In the **History** section, Kaspersky MLAD displays a graph of tags received from the monitored asset for which the selected incident was registered. The graph displays data on the preset named Tags for event #N (N represents the incident number in the **Incidents** section), which is generated for the date and time when the selected incident was registered. This preset includes the tags that led to incident registration. Depending on the type of detector that registered an incident, this may involve the following tags:

   - Tags whose actual values were deemed the most anomalous by the ML model, if the incident was registered by the Forecaster Detector.
   - Tags included in a diagnostic rule and the value obtained as a result of the operation of this rule, if the incident was registered by the Rule Detector.
   - A tag whose value was outside of the set blocking thresholds, if the incident was registered by the Limit Detector.

   If necessary, you can select a different preset for displaying data received from the monitored asset at the moment when the incident was registered. The graph uses a vertical blue dashed line to indicate the date and time when the incident was registered.

   Example tag graph in the History section ?.

The tag graph is displayed in the upper part of the **History** section. The MSE graph is displayed in the lower part of the **History** section.



Sep_underflow_stream10 [26]
Separator Underflow (stream 10)
Date and time: **13.11.2023 23:39:49**
Dimension: **m3/hr**
● Observed: **25.141**
● Prediction:
- transformer@TEP Imported: **25.278**

Tag graph in the **History** section

2 Configuring how data is displayed on a graph in the History section

In the **History** section, you can enable the display of predicted tag values. This lets you assess the difference between actual tag values and predicted tag values. Enabling the display of predicted values will also let you view values obtained as a result of the work of diagnostic rules. Tag information (name, numerical ID, description, unit of measurement, time, and tag value) is displayed whenever you move your mouse cursor over a tag graph. You can also enable display of the tag name and description for each tag graph.

3 Configuring the time settings for displaying data in the History section

When studying the behavior of tags, you can change the scale of the time axis or move forward or backward in time through graphs. When displaying shorter time intervals on tag graphs, the **History** section may show more details of the behavior of tags that had been averaged when a tag graph for a longer period was displayed.

4 Changing the vertical boundaries for displaying data in the History section

The vertical scale of each graph is selected by default based on the minimum and maximum values of a tag in the displayed area. You can control the scale of graphs according to the scale of values on the vertical axis by using one of the following methods:

- If minimum and maximum permissible values (blocking thresholds) are defined for a tag, enable the **Always display blocking threshold** function.

  If a tag value is within the permissible range, the vertical scale of the graph will be fixed by limit lines derived from the lower and upper thresholds of the tag graph. If the tag values go beyond the specified blocking thresholds, the vertical scale will be automatically changed to display the tag values exceeding the thresholds.

- In the tag properties, set the permissible boundaries for displaying tag values on graphs.

  If tag values go beyond the defined boundaries, they will not be displayed on the tag graph. The permissible boundaries for displaying tag values take priority over the display of blocking thresholds, even if the **Always display blocking threshold** function is enabled.

Adding a status, cause, expert opinion or note to an incident or incident group

Kaspersky MLAD lets you add an expert opinion or note to a registered incident.

An expert opinion is normally added by an expert (process engineer or ICS specialist) and may contain an incident analysis or recommendations on resolving a problem that is indicated by an identified incident. An expert opinion can be added to an individual incident or to a group of incidents. If expert opinions were previously added to incidents that are later put into a group, these opinions will also be displayed in the group (linked to each specific incident). When incidents are regrouped, the expert opinion for an incident migrates together with the incident to the new group.

Notes are intended to aid discussions between experts or operators of facilities regarding recommended actions for analysis, investigation, and remediation of an incident. Each note includes information stating who added the note and when it was added.

You can also add the cause of the incident and the incident status determined by the expert based on the incident analysis results. A status can be assigned to an individual incident or to a group of incidents. When changing the status of a group of incidents, Kaspersky MLAD changes the status of the incidents that are part of this group.

> Before adding a cause, status, note or expert opinion, you must conduct an analysis of the registered incident.

To add an expert opinion, status, cause, or note to an incident:

1. In the main menu, select the **Incidents** section.

2. If necessary, change the incident status by selecting one of the following statuses from the **Status** drop-down list: **Under review**, **Decision pending**, **Instructions issued**, **Problem closed**, **Cause unknown**, **Ignore**, or **False positive**.

   By default, an incident is assigned the **Unknown** status. If necessary, the system administrator can create, edit, or delete statuses of incidents.

3. To display detailed technical specifications, click the right arrow (›) next to the relevant incident. In the details area that opens, you can do the following:

   - If you need to add the cause of an incident, use the **Incident cause** field to select the cause of the incident.

     If necessary, the system administrator can create, edit, or delete causes of incidents.

   - If you want to add an expert opinion based on an analysis of a registered incident, click the **Edit expert opinion** (✎) icon on the right of the **Expert opinion** field. In the field that opens, enter the opinion, and press **ENTER**.

     The expert opinion will be added to the selected incident and will appear in the incidents table in the **Incidents** section.

   - If you need to add a note to an incident, enter your message in the **Note** field and click the **Add note** button.

     You can provide a message up to 512 characters long.

The status, cause, expert opinion, and note will be added to the incident and will be available to other users when viewing this incident.

When two or more similar incidents are detected, Kaspersky MLAD automatically combines them into a group. The group name is also automatically assigned in the format Group #N (N is replaced by the sequence number of the group). You can edit the group name, change the status of an incident group, and edit the expert opinion containing recommendations for analyzing similar events, for example.

To add a status and expert opinion to a group of incidents:

1. In the main menu, select the **Incidents** section and click **Groups**.
2. If necessary, change the incident group status by selecting one of the following statuses from the **Status** drop-down list: **Under review**, **Decision pending**, **Instructions issued**, **Problem closed**, **Cause unknown**, **Ignore**, or **False positive**.

   When changing the status of a group of incidents, Kaspersky MLAD changes the status of the incidents that are part of this group. By default, a group of incidents is assigned the **Unknown** status.

   If necessary, the system administrator can create, edit, or delete statuses of incidents.
3. In the incident groups table, double-click the row of the incident group.

   The **Edit group** window opens.

   You can also change the group on the **Incidents** tab. To do so, select the required group in the **Group** filter, and in the expert opinion section for the group, which is displayed above the incidents table, click the **Edit** button.
4. To change the name of the incident group, enter a new name for the group in the **Group name** field.
5. In the **Expert opinion** field, enter the text of the expert opinion (for example, recommendations for analyzing similar incidents).
6. Click the **Save** button.

The status and expert opinion will be changed for the incident group and can now be viewed by other users in the **Groups** table in the **Incidents** section.

Exporting incidents to a file

Incidents registered for a specific period in Kaspersky MLAD can be exported to an XLSX file.

To save incidents registered for a specific period to a file:

1. In the main menu, select the **Incidents** section.
2. In the upper part of the opened page, select the start and end dates of the period.
3. Click the **Export** button.
4. Select a directory to save on your local drive, and save the file.

Incidents registered for the selected period in Kaspersky MLAD will be saved to an XLSX file on the local drive. The XLSX file can be opened in Microsoft® Excel®.

Managing ML models

This section provides instructions on working with ML models, ML model templates and markups.

ML models, templates of ML models and markups are functional elements of the monitored asset hierarchical structure. The hierarchical structure is displayed as an asset tree.

In Kaspersky MLAD, ML models can be imported, created manually, copied, or created based on a template. After adding and training an ML model in Kaspersky MLAD, you can publish it. You can also run a historical or stream inference for the trained or published ML model, and view the data flow graph in the ML model.

In the **Models** section, you can create markups for generating learning indicators or inference indicators. If necessary, you can edit or delete markups.

Scenario: working with ML models

This section describes the sequence of actions required to work with ML models.

The scenario for working with ML models consists of the following steps:

1. **Adding an ML model**

   You can add an ML model to Kaspersky MLAD in one of the following ways:

   - Upload an ML model created by Kaspersky specialists or by a certified integrator as part of the *Kaspersky MLAD Model-building and Deployment Service*. After an ML model is uploaded, it must be activated.
   - Manually create an ML model. Add neural network elements and/or elements based on diagnostic rules to the created ML model.
   - Create an ML model from a template. Create a template based on the relevant ML model in advance. If the original ML model used for the template was manually created, you can add neural network elements and/or elements based on diagnostic rules to the new ML model.
   - Clone a previously added ML model. When cloning an ML model that was created manually or from a template based on a manually created ML model, you can add neural network elements and/or the elements based on diagnostic rules to the cloned ML model.

2. **Adding markups**

   If you need to define specific time intervals for the data that an ML model can use for training or inference, create markups. To generate an inference indicator, specify the created markup in the settings of the corresponding ML model.

3. **Training ML model elements**

   The ML model needs to be trained before you can run inference on it. To do this, all neural network elements within the ML model need to be pretrained. ML model elements based on diagnostic rules are considered to be already trained.

   An ML model uploaded to Kaspersky MLAD has been previously trained by Kaspersky Lab experts or a certified integrator. ML models that are created from a template of an imported ML model or by cloning an imported ML model are also considered to be already trained. If necessary, you can change their training parameters and retrain the neural network elements.

   To generate a learning indicator, specify the created markup in the learning parameters of the neural network element.

4. **Preparing an ML model for publication**

   After its training is finished, prepare the ML model for publication. An ML model ready for publishing cannot be modified.

5. **Publishing an ML model**

   After preparing the ML model for publication, notify the officer responsible for publishing the ML model that the ML model is ready, or publish the ML model if you have the required permissions. If necessary, the system administrator can create a role that has the right to publish ML models and assign this role to the relevant employee.

6. **Starting ML model inference**

   Start inference of the ML model. During the inference process, the ML model analyzes telemetry data and registers incidents.

   ML model inference can be run on a published ML model as well as on a trained ML model.

Working with markups

This section provides information on working with markups.

In the **Models** section, you can create, modify, and delete markups. If required, you can view the graph to see the data time intervals that the ML model will use for training and/or inference.

Markups are used as training or inference indicators to point to data time intervals that the ML model can use for training or inference. To generate an inference indicator ?, you can select previously created markups when creating or modifying ML model settings. To generate a learning indicator ?, you can select previously created markups when configuring the training settings of neural network elements of the ML model.

Creating markup

You can use markup to generate learning indicators or inference of the ML model.

To create markup:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the name of the asset for which you want to create a markup, open the vertical menu **...** and select **Create markup**.

   A list of options appears on the right.
3. Specify the name of the markup in the **Name** field.
4. Enter a description for the markup in the **Description** field.
5. In the **Grid step (sec)** field, specify a UTG period for markup in seconds expressed as a decimal.
6. In the **Markup color** field, select a color that will be used to highlight data intervals selected by the markup.
7. If necessary, use the toggle switch to turn on the **Treat inconclusive result as positive** option.

   If Kaspersky MLAD cannot unequivocally evaluate the fulfillment of criteria specified in the **Time filter** and **Tag conditions** settings blocks, for example, due to the absence of observations for tags, the application will consider specified criteria to be fulfilled when this option is enabled.
8. In the **Time filter** settings block, do the following:

   a. Click the **Add interval** button.

   b. In the **Interval type** drop-down list, select one of the following time interval types:

      - **Fixed**. If you select this type of interval, specify the days of the week and the time interval during which the input data must be validated according to the specified criteria.

        You can specify only the beginning or the end of a single interval.

      - **Recurrent**. If you select this type of interval, specify the years, dates, days of the week, and daily time interval for periodically validating input data according to the specified criteria.

   You can add one or more time intervals.

9. To add tag behavior criteria, do the following:

   a. In the **Tag conditions** settings block, click the **Condition** button.

   b. In the **Tag** drop-down list, select the tag for which to add a tag behavior criterion.

      If you want to exclude the selected criterion from the condition block that you are adding, click **NOT** to the left of the selected tag. The **NOT** caption in the button will be highlighted in bold.

      For example, click **NOT** to add a condition that contains no steps with the specified settings.

   c. In the **Behavior** drop-down list, select one of the following tag behaviors that must be tracked:

      - **Over**: the tag value exceeds the specified threshold.

      - **Below**: the tag value falls below the specified threshold.

      - **Rising**: the trendline of tag values is increasing.

      - **Falling**: the trendline of tag values is decreasing.

      - **Level**: there are no pronounced changes in the trendline of tag values.

      - **Step change**: the trendline of the selected tag is displaying abrupt upward or downward shifts.

      - **Flat**: the selected tag is transmitting the same value.

      - **Spread**: abrupt changes in the spread of values are being observed around the trendline of the selected tag.

   d. In the **Window** field, specify an interval for analyzing the behavior of tags in the UTG steps.

   e. Depending on the value selected for **Behavior**, do one of the following:

      - If you selected **Over** or **Below**, use the **Threshold** field to specify the tag threshold value, and specify the minimum number of times the threshold value can be breached in a separate window in the **Minimum violations** field.

      - If you selected **Rising**, **Falling**, or **Level**, use the **Threshold slope** field to specify the trend slope percentage value that must be exceeded for the trend to be considered as growing or falling, and specify the time interval between adjacent trend estimates in the **Evaluation period** field.

        By default, the **Threshold slope** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine the trend direction automatically.

By default, the **Evaluation period** setting has a value of `1`. With this value, the trend is estimated at each UTG node.

- If you selected **Step change**, use the **Minimum change** field to specify the minimum shift value for the tag trendline, and select one of the following tag value change directions from the **Direction** drop-down list: **Any**, **Up** or **Down**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

- If you selected **Flat**, use the **Value** field to specify the value that the tag should transmit, and specify the maximum tag value spread in the **Spread** field.

  By default, the **Value** setting is not defined. If the setting is not defined, any repeating tag value triggers the criterion.

- If you selected **Spread**, use the **Minimum change** field to specify the minimum value by which the tag value spread around the trendline can change, and select one of the following spread change directions in the **Direction** drop-down list: **Any**, **Flare**, or **Shrink**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

  The tag behavior criterion is met when the tag spread around the trendline increases and/or decreases.

f. To add a tag behavior criterion to a condition block, click the plus sign at the bottom of the condition block and repeat steps 9b through 9e.

g. If the block contains more than one tag behavior criterion, select one of the following logical operators between the criterion rows:

- **AND** if you need to track both criteria in the markup.
- **OR** if you need to track one of the defined criteria in the markup.

10. If you need to check whether the fulfillment of a pre-condition triggered the fulfillment of a post-condition, do the following:

a. Add one of the following temporal operators:

- **Wait** if you need to generate the result of the criteria check in the last node of the maximum waiting interval.
- **If ahead** if you need to generate the result of the criteria check at the time of a pre-condition check.

The **Wait** and **If ahead** buttons are available after adding at least one condition.

A *precondition* is a block of conditions preceding the temporal operator. A *postcondition* is a block of conditions following a temporal operator.

The precondition block is checked in the current UTG node.

Markup with an **If ahead** temporal operator can be used in learning indicators only.

b. In the **Recess (steps)** field, specify the following time intervals:

- **from**: the interval between the current UTG node and the first future UTG node, in which the post-condition block is checked (minimum waiting interval).
- **to**: the interval between the current UTG node and the last future UTG node, in which the post-condition block is checked (maximum waiting interval).

The post-condition block is checked in the UTG nodes between the minimum and maximum waiting intervals.

c. In the **Check** drop-down list, select one of the following group operators:

- To check the fulfillment of tag behavior criteria from the post-conditions block in all UTG nodes between the minimum and maximum waiting intervals, select the **All steps** group operator.
- To check the fulfillment of tag behavior criteria from the post-conditions block in at least one UTG node between the minimum and maximum waiting intervals, select the **Any step** group operator.

If the **Wait** temporal operator is added, the criteria check result is determined in the last node of the maximum waiting interval. If the check of the precondition block in the current UTG node gave a negative result (FALSE) or an undefined result (UNDEFINED), the same value will be the result of the check of the post-condition block. If the check of the precondition block in the current UTG node gave a positive result (TRUE), then the check of the post-condition block is performed in each UTG node between the minimum and maximum waiting interval. The result of the check is determined by the fulfillment of the condition depending on the selected group operator: **All steps** or **Any step**. If more than one condition check is performed using the **Wait** temporal operator, the result of the previous temporal condition check is the precondition for each subsequent check of the **Wait** temporal condition.

If the **If ahead** temporal operator is added, the criteria check result is generated at the time of the precondition check.

11. Select one of the following logical operators between markup blocks:

    - **AND** if you need to track the tag behavior criteria in both blocks of conditions.
    - **OR** if you need to track the tag behavior criteria in only one of the blocks of conditions.

12. In the upper-right corner of the window, click the **Save** button.

The new markup will be displayed in the **Markups** group of the asset tree. The **Markups** group is created automatically and displayed as part of the selected section of the asset tree.

Viewing the markup chart

After creating markup, you can view data time intervals selected by the markup on the graph.

To view the markup chart:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the markup whose chart you want to view.

   A list of options appears on the right.
3. Click the **On graph** button.

   A panel with the markup chart appears on the right.
4. Select the relevant preset from the **Preset** drop-down list.
5. If necessary, in the **Markups** field, select the markups for displaying data intervals.
6. If you need to select a date and time for displaying the data, do one of the following:

   - In the **Graph center** field, select the date and time for which you want to display data in the chart.

The vertical black dotted line will indicate the selected date and time (in the center of the chart).

- Click the **New graph center** icon (⊙), which is located to the left of the time axis, and select the necessary point on the time axis.

  The selected point will become the new center of the graph. The vertical black dashed line will indicate the new date and time.

7. If you need to select a time interval for displaying data on the chart, do one of the following:

   - If you need to display data for a fixed time interval, select the relevant time interval from the **Scale** drop-down list. The following time intervals are available by default:

     - 1, 5, 10, 15, and 30 minutes
     - 1, 3, 6, and 12 hours
     - 1, 2, 15, and 30 days
     - 3 and 6 months
     - 1, 2, and 3 years

     If necessary, the system administrator can create, edit, or delete time intervals.

   - To display data for a custom time interval, click the **New interval** (ılı) icon to the left of the time axis, select the required interval on the time axis, and click the **Apply** button. If you need to change the scale again, repeat this step.

The chart will show the data intervals in the colors specified for the selected markups.

Modifying the markup

You can edit the markup settings.

To edit markup:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the markup that you want to edit.

   A list of options appears on the right.
3. Click the **Edit** button.
4. In the **Name** field, specify a new name for the markup.
5. Enter a new description for the markup in the **Description** field.
6. In the **Grid step (sec)** field, specify a UTG period for markup in seconds expressed as a decimal.
7. In the **Markup color** field, select a color that will be used to highlight data intervals selected by the markup.
8. If necessary, use the toggle switch to turn on the **Treat inconclusive result as positive** option.

If Kaspersky MLAD cannot unequivocally evaluate the fulfillment of criteria specified in the **Time filter** and **Tag conditions** settings blocks, for example, due to the absence of observations for tags, the application will consider specified criteria to be fulfilled when this option is enabled.

9. If you want to edit the markup time intervals in the **Time filter** settings block, do the following:

   a. In the **Interval type** drop-down list, select one of the following time interval types:

   - **Fixed**. If you select this type of interval, specify the days of the week and the time interval during which the input data must be validated according to the specified criteria.

     You can specify only the beginning or the end of a single interval.

   - **Recurrent**. If you select this type of interval, specify the years, dates, days of the week, and daily time interval for periodically validating input data according to the specified criteria.

   b. If you want to add an interval, click the **Add interval** button and complete step 9a.

   c. If you want to delete an interval, move the mouse cursor over the row with the required interval and click the **Delete interval** (✕) icon.

   You can add one or more time intervals.

10. To edit a tag behavior condition, do the following:

    a. In the **Tag** drop-down list, select the tag for which to add a tag behavior criterion.

    If you want to exclude the selected criterion from the condition block that you are adding, click **NOT** to the left of the selected tag. The **NOT** caption in the button will be highlighted in bold.

    For example, click **NOT** to add a condition that contains no steps with the specified settings.

    b. In the **Behavior** drop-down list, select one of the following tag behaviors that must be tracked:

    - **Over**: the tag value exceeds the specified threshold.
    - **Below**: the tag value falls below the specified threshold.
    - **Rising**: the trendline of tag values is increasing.
    - **Falling**: the trendline of tag values is decreasing.
    - **Level**: there are no pronounced changes in the trendline of tag values.
    - **Step change**: the trendline of the selected tag is displaying abrupt upward or downward shifts.
    - **Flat**: the selected tag is transmitting the same value.
    - **Spread**: abrupt changes in the spread of values are being observed around the trendline of the selected tag.

    c. In the **Window** field, specify the number of UTG steps.

    d. Depending on the value selected for **Behavior**, do one of the following:

    - If you selected **Over** or **Below**, use the **Threshold** field to specify the tag threshold value, and specify the minimum number of times the threshold value can be breached in a separate window in the **Minimum violations** field.

- If you selected **Rising**, **Falling**, or **Level**, use the **Threshold slope** field to specify the trend slope percentage value that must be exceeded for the trend to be considered as growing or falling, and specify the time interval between adjacent trend estimates in the **Evaluation period** field.

  By default, the **Threshold slope** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine the trend direction automatically.

  By default, the **Evaluation period** setting has a value of `1`. With this value, the trend is estimated at each UTG node.

- If you selected **Step change**, use the **Minimum change** field to specify the minimum shift value for the tag trendline, and select one of the following tag value change directions from the **Direction** drop-down list: **Any**, **Up** or **Down**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

- If you selected **Flat**, use the **Value** field to specify the value that the tag should transmit, and specify the maximum tag value spread in the **Spread** field.

  By default, the **Value** setting is not defined. If the setting is not defined, any repeating tag value triggers the criterion.

- If you selected **Spread**, use the **Minimum change** field to specify the minimum value by which the tag value spread around the trendline can change, and select one of the following spread change directions in the **Direction** drop-down list: **Any**, **Flare**, or **Shrink**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

  The tag behavior criterion is met when the tag spread around the trendline increases and/or decreases.

e. To add a tag behavior criterion to a condition block, click the plus sign at the bottom of the condition block and repeat steps 10a through 10d.

f. If the block contains more than one tag behavior criterion, select one of the following logical operators between the criterion rows:

- **AND** if you need to track both criteria in the markup.
- **OR** if you need to track one of the defined criteria in the markup.

g. To delete a tag behavior criterion from a condition block, hover over the row with the required condition and click the cross icon (✕).

11. If you want to edit the conditions of the temporal operator **Wait** and/or **If ahead**, do the following:

a. In the **Recess (steps)** field, specify the following time intervals:

- **from**: the interval between the current UTG node and the first future UTG node, in which the post-condition block is checked (minimum waiting interval).
- **to**: the interval between the current UTG node and the last future UTG node, in which the post-condition block is checked (maximum waiting interval).

The post-condition block is checked in the UTG nodes between the minimum and maximum waiting intervals.

b. In the **Check** drop-down list, select one of the following group operators:

- To check the fulfillment of tag behavior criteria from the post-conditions block in all UTG nodes between the minimum and maximum waiting intervals, select the **All steps** group operator.

- To check the fulfillment of tag behavior criteria from the post-conditions block in at least one UTG node between the minimum and maximum waiting intervals, select the **Any step** group operator.

If the **Wait** temporal operator is added, the criteria check result is determined in the last node of the maximum waiting interval. If the check of the precondition block in the current UTG node gave a negative result (FALSE) or an undefined result (UNDEFINED), the same value will be the result of the check of the post-condition block. If the check of the precondition block in the current UTG node gave a positive result (TRUE), then the check of the post-condition block is performed in each UTG node between the minimum and maximum waiting interval. The result of the check is determined by the fulfillment of the condition depending on the selected group operator: **All steps** or **Any step**. If more than one condition check is performed using the **Wait** temporal operator, the result of the previous temporal condition check is the precondition for each subsequent check of the **Wait** temporal condition.

If the **If ahead** temporal operator is added, the criteria check result is generated at the time of the precondition check.

12. Select one of the following logical operators between markup blocks:

    - **AND** if you need to track the tag behavior criteria in both blocks of conditions.
    - **OR** if you need to track the tag behavior criteria in only one of the blocks of conditions.

13. In the upper-right corner of the window, click the **Save** button.

Removing markup

You can delete markup if it is not used for training or inference of any ML model.

To delete markup:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the markup that you want to delete.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the trash bin icon (🗑).
4. In the window that opens, confirm the deletion of the markup.

Working with imported ML models

This section provides information about working with imported ML models and their elements.

ML models can be provided by Kaspersky specialists or certified integrators within the *Kaspersky MLAD Model-building and Deployment Service*. Such ML models must be uploaded to Kaspersky MLAD and activated. You cannot create new elements for an imported ML model, or delete existing elements.

Upon uploading into Kaspersky MLAD the ML model is already trained. If necessary, you can additionally train the neural network elements as part of the uploaded ML model before publishing it and/or executing its inference.

Uploading an ML model

If the ML model was created by Kaspersky specialists or a certified integrator, you can load this ML model into Kaspersky MLAD.

Kaspersky MLAD may slow down its operation when uploading an ML model whose size exceeds 1 GB.

System administrators and users who have the **Upload models** permission from the **Manage ML models** group of rights can upload ML models.

To upload an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the name of the asset for which the ML model is to be imported, open the vertical menu **...** and select **Import model**.
3. In the opened window, select the ML model file.

   An ML model file is provided as a TAR archive with a maximum size of 1.5 GB.

The ML model will be uploaded to Kaspersky MLAD. The new ML model displays in the **Models** group of the asset tree. The **Models** group is created automatically and displayed as part of the selected section of the asset tree. The **Models** group contains the **Neural networks** and **Rules** subgroups for storing ML model elements based on neural networks and diagnostic rules.

After being uploaded, the ML model is assigned the *Not activated* status. The ML model must be activated. If you upload an ML model that was previously activated and then deleted, you do not need to reactivate the ML model.

Activating an imported ML model

After an ML model prepared by Kaspersky specialists or a certified integrator has been uploaded into Kaspersky MLAD, it must be activated.

If the ML model activation code is lost, send a request to Kaspersky to receive a new code.

System administrators and users who have the **Activate models** permission from the **Manage ML models** group of rights can activate imported ML models.

To activate an imported ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the imported ML model.

   The details area appears on the right.

3. In the **Model activation code** field, enter the code received from Kaspersky personnel, and click the **Activate** button in the upper right part of the window.

ML model is activated. It will be assigned the *Trained* status. You can to start ML model inference to begin the analysis of telemetry data received from the monitored asset.

Changing the parameters of an element of an imported ML model

You can change some parameters of an element of an imported ML model.

System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can edit the settings of elements of imported ML models.

To change the parameters of an imported ML model element:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model element that you want to change.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the **Edit** button.
4. In the **Name** field, specify the name of the ML model element.
5. Enter a description for the ML model element in the **Description** field.
6. If necessary, in the **General element settings** settings block, do the following:

   a. In the **Reminder period (sec)** field, specify the period in seconds, upon reaching which the ML model will generate a repeated incident if anomalous behavior is retained in each UTG node.

      The default value of this setting is `0`, which corresponds to no reminders.

   b. In the **Period of recurring alert suppression (sec)** field, specify the period in seconds during which the ML model does not log repeated incidents for the same element.

      The default value of this setting is `0` (repeat incidents not suppressed).

   c. In the **Incident status** drop-down list, select a status to be automatically assigned to incidents logged by the ML model element.

   d. In the **Incident cause** drop-down list, select the cause to be automatically set for incidents logged by the ML model element.

   e. In the **Color of incident dot indicators** field, select the color of the indicator points of the incidents logged by the ML model element on the graphs in the **Monitoring** and **History** sections.

   f. In the **Detection threshold** field, specify a prediction error threshold value upon reaching which an incident is logged.

      The detection threshold value was set after training an element of the imported ML model. Modifying this setting changes detector sensitivity.

g. In the **Expert opinion** field, specify the expert opinion to be automatically created for incidents logged by the ML model element.

7. In the upper-right corner of the window, click the **Save** button.

Working with manually created ML models

This section provides information about working with manually created ML models and their elements.

If you create an ML model manually, you can add elements of ML models based on neural networks and/or diagnostic rules, modify or delete them.

The ML model needs to be trained before you can run inference on it. To do this, all neural network elements within the ML model need to be pretrained. If necessary, you can view the training results of the neural network elements. Elements based on diagnostic rules are considered as trained.

You can also start inference after publishing the ML model. After inference is started, Kaspersky MLAD will register incidents.

Creating an ML model

System administrators and users who have the **Create models** permission from the **Manage ML models** group of rights can create ML models.

To create an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the name of the asset for which you want to create an ML model, open the vertical menu **...** and select **Create model**.

   A list of options appears on the right.
3. In the **Name** field, specify the ML model name.

   The ML model name must not be longer than 100 characters.
4. In the **Description** field, specify the ML model description.
5. If you need to apply markups when selecting data for ML model inference, select the required markups under **Inference indicator**.
6. To view the data that will be selected by the markups, click **On graph**.

   Markups are displayed in the colors selected when they were created.
7. In the upper-right corner of the window, click the **Save** button.

The new ML model displays in the **Models** group of the asset tree. The **Models** group is created automatically and displayed as part of the selected section of the asset tree. The **Models** group contains the **Neural networks** and **Rules** subgroups for storing ML model elements based on neural networks and diagnostic rules.

The ML model is assigned the *Draft* status.

Adding a neural network element to an ML model

System administrators and users who have the **Create models** permission from the **Manage ML models** group of rights can add ML model elements.

To add a neural network element to an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the **Neural networks** group within the ML model to which you want to add a neural network element, open the vertical menu **...** and select **Create element**.

   A list of options appears on the right.
3. In the **Name** field, specify the name of the ML model element.
4. Enter a description for the ML model element in the **Description** field.
5. In the **General element settings** settings block, do the following:
   1. In the **Reminder period (sec)** field, specify the period in seconds, upon reaching which the ML model will generate a repeated incident if anomalous behavior is retained in each UTG node.

      The default value of this setting is `0`, which corresponds to no reminders.
   2. In the **Period of recurring alert suppression (sec)** field, specify the period in seconds during which the ML model does not log repeated incidents for the same element.

      The default value of this setting is `0` (repeat incidents not suppressed).
   3. In the **Grid step (sec)** field, specify the element's UTG period in seconds expressed as a decimal.
   4. In the **Incident status** drop-down list, select a status to be automatically assigned to incidents logged by the ML model element.
   5. In the **Incident cause** drop-down list, select the cause to be automatically set for incidents logged by the ML model element.
   6. In the **Color of incident dot indicators** field, select the color of the indicator points of the incidents logged by the ML model element on the graphs in the **Monitoring** and **History** sections.
   7. In the **Detection threshold** field, specify a prediction error threshold value upon reaching which an incident is logged.
   8. In the **Expert opinion** field, specify the expert opinion to be automatically created for incidents logged by the ML model element.
6. Select one of the following ML model neural network element architectures: **Dense**, **RNN**, **CNN**, **TCN**, or **Transformer**.
7. If you need to specify the architecture parameters of a neural network element and the power exponent and smoothing value of the cumulative prediction error, use the toggle switch to enable **Advanced neural network settings**.

8. In the **Main settings** block, do the following:

   a. In the **Input tags** drop-down list, select one or more tags that serve as the source data for predicting the values of the output tags.

   b. In the **Output tags** drop-down list, select one or several tags whose behavior is predicted by the model element.

   c. If extended setup mode is enabled, use the **MSE power exponent** field to specify the cumulative prediction error power exponent in decimal format.

   d. If extended setup mode is enabled, use the **Smoothing factor** field to specify the cumulative prediction error smoothing value in decimal format.

9. In the **Window settings** settings block, do the following:

   a. In the **Input window (steps)** field, specify the size of the input value window, from which the ML model element predicts the output values.

   b. In the **Output window offset** field, specify the number of steps by which the beginning of the output window will be shifted relative to the beginning of the input window.

   c. In the **Output window (steps)** field, specify an output tag prediction length calculated from the input tags on the input window.

10. If you are adding a neural network element with a dense architecture, do the following:

    a. In the **Multipliers for calculating number of neurons per layer** field, provide the factors, separated by a comma without spaces, by which to multiply the number of input tags to calculate the number of neurons per layer of the ML model element.

    b. In the **Activation function per layer** field, specify one of the following activation functions on each layer of an ML model element separated by a comma without spaces:

    - `relu`: A non-linear activation function that converts an input value to a value between `0` and positive infinity.

    - `selu`: A monotonically increasing function that enables normalization based on the central limit theorem.

    - `linear`: A linear function that is a straight line proportional to the input data.

    - `sigmoid`: A non-linear function that converts input values to values between `0` and `1`.

    - `tanh`: A hyperbolic tangent function that converts input values to values between `-1` and `1`.

    - `softmax`: A function that converts a vector of values to a probability distribution that adds up to `1`.

    The default value of this setting is `relu,relu,relu`.

11. If you are adding a neural network element with an RNN architecture, do the following:

    a. In the **GRU neurons per layer** field, specify the number of GRU neurons on layers separated by a comma without spaces.

    The default value of this parameter is `40,40`.

b. In the **Number of neurons in TimeDistributed layer** field, specify the number of neurons distributed in time on the layers of the decoder separated by a comma without spaces.

   The default value of this parameter is `40,20`.

12. If you are adding a neural network element with an CNN architecture, do the following:

    a. In the **Filter size per layer** field, specify the size of the filters for each layer of the element separated by a comma without spaces.

    The default value of this parameter is `2,2,2`.

    b. In the **Filters per layer** field, specify the number of filters for each layer of the ML model element separated by a comma without spaces.

    The default value of this parameter is `50,50,50`.

    c. In the **MaxPooling window size per layer** field, specify the maximum sampling window size on each layer separated by a comma without spaces.

    The default value of this parameter is `2,2,2`.

    d. In the **Number of neurons in decoder** field, specify the number of neurons on the layers of the decoder.

13. If you are adding a neural network element with an TCN architecture, do the following:

    a. In the **Regularization** field, specify the regularization coefficient in decimal format to prevent overfitting of the ML model element.

    The default value of this parameter is `0.1`.

    b. In the **Size of filters** field, specify the size of the filters for the ML model element.

    The default value of this parameter is `2`.

    c. In the **Dilation per layer** field, specify the exponential expansion values of the output data on the layers as a comma-separated list.

    The default value of this parameter is `1,2,4`.

    d. In the **Activation function** drop-down list, select one of the following activation functions:

    - **linear**: A linear activation function whose result is proportional to the input value.
    - **relu**: A non-linear activation function that converts an input value to a value between zero and positive infinity. If the input value is less than or equal to zero, the function returns a value of zero; otherwise, the function returns the input value.

    The default value of this parameter is **linear**.

    e. In the **Number of stacks of residual blocks** field, specify the number of encoders.

    The default value of this parameter is `1`.

    f. In the **Decoder layer type** field, select one of the following types of layer to precede the output layer:

    - **TimeDistributedDense** (default): A fully connected architecture layer.
    - **GRU**: A layer with a recurrent architecture.

14. If you are adding a neural network element with a transformer architecture, do the following:

a. In the **Encoder regularization** field, specify the regularization coefficient in the encoder in decimal format.

   The default value of this parameter is `0.01`.

b. In the **Number of attention heads** field, specify the number of attention heads.

   The default value of this parameter is `1`.

c. In the **Number of encoders** field, specify the number of encoders.

   The default value of this parameter is `1`.

d. In the **Multipliers for calculating number of neurons per layer** field, provide the factors, separated by a comma without spaces, by which to multiply the number of input tags to calculate the number of neurons in the decoding layers.

15. In the upper-right corner of the window, click the **Save** button.

The new ML model element will be displayed in the **Neural networks** group within the selected ML model in the asset tree.

The ML model is assigned the *Draft* status. Before running inference of an ML model, you must train all of its neural network elements.

Modifying a neural network element of the ML model

You can edit the settings of a neural network element of the ML model.

System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can edit elements of ML models.

To edit a neural network element of an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the neural network element that you want to edit.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the **Edit** button.
4. In the **Name** field, specify a new name for the ML model element.
5. In the **Description** field, specify a new description for the ML model.
6. If necessary, in the **General element settings** settings block, do the following:

   a. In the **Reminder period (sec)** field, specify the period in seconds, upon reaching which the ML model will generate a repeated incident if anomalous behavior is retained in each UTG node.

      The default value of this setting is `0`, which corresponds to no reminders.

   b. In the **Period of recurring alert suppression (sec)** field, specify the period in seconds during which the ML model does not log repeated incidents for the same element.

      The default value of this setting is `0` (repeat incidents not suppressed).

c. In the **Grid step (sec)** field, specify the element's UTG period in seconds expressed as a decimal.

d. In the **Incident status** drop-down list, select a status to be automatically assigned to incidents logged by the ML model element.

e. In the **Incident cause** drop-down list, select the cause to be automatically set for incidents logged by the ML model element.

f. In the **Color of incident dot indicators** field, select the color of the indicator points of the incidents logged by the ML model element on the graphs in the **Monitoring** and **History** sections.

g. In the **Detection threshold** field, specify a prediction error threshold value upon reaching which an incident is logged.

h. In the **Expert opinion** field, specify the expert opinion to be automatically created for incidents logged by the ML model element.

7. If necessary, edit the architecture of the neural network element.

   Kaspersky MLAD supports the following ML model neural network element architectures: **Dense**, **RNN**, **CNN**, **TCN**, or **Transformer**.

8. If you need to change the architecture parameters of a neural network element and the power exponent and smoothing value of the cumulative prediction error, use the toggle switch to enable **Advanced neural network settings**.

9. If necessary, in the **Main settings** settings block, do the following:

   a. In the **Input tags** drop-down list, select one or more tags that serve as the source data for predicting the values of the output tags.

   b. In the **Output tags** drop-down list, select one or several tags whose behavior is predicted by the model element.

   c. If extended setup mode is enabled, use the **MSE power exponent** field to specify the cumulative prediction error power exponent in decimal format.

   d. If extended setup mode is enabled, use the **Smoothing factor** field to specify the cumulative prediction error smoothing value in decimal format.

10. If necessary, in the **Window settings** settings block, do the following:

    a. In the **Input window (steps)** field, specify the size of the input value window, from which the ML model element predicts the output values.

    b. In the **Output window offset** field, specify the number of steps by which the beginning of the output window will be shifted relative to the beginning of the input window.

    c. In the **Output window (steps)** field, specify an output tag prediction length calculated from the input tags on the input window.

11. If you have selected a neural network element with a dense architecture, do the following:

    a. In the **Multipliers for calculating number of neurons per layer** field, provide the multipliers, separated by a comma without spaces, by which to multiply the number of input tags to calculate the number of neurons in the ML model element layers.

b. In the **Activation function per layer** field, specify one of the following activation functions on each layer of an ML model element separated by a comma without spaces:

- `relu`: A non-linear activation function that converts an input value to a value between `0` and positive infinity.
- `selu`: A monotonically increasing function that enables normalization based on the central limit theorem.
- `linear`: A linear function that is a straight line proportional to the input data.
- `sigmoid`: A non-linear function that converts input values to values between `0` and `1`.
- `tanh`: A hyperbolic tangent function that converts input values to values between `-1` and `1`.
- `softmax`: A function that converts a vector of values to a probability distribution that adds up to `1`.

The default value of this setting is `relu,relu,relu`.

12. If you are adding a neural network element with an RNN architecture, do the following:

a. In the **GRU neurons per layer** field, specify the number of GRU neurons on layers separated by a comma without spaces.

The default value of this parameter is `40,40`.

b. In the **Number of neurons in TimeDistributed layer** field, specify the number of neurons distributed in time on the layers of the decoder separated by a comma without spaces.

The default value of this parameter is `40,20`.

13. If you have selected a neural network element with a CNN architecture, do the following in the **CNN architecture settings** settings block:

a. In the **Filter size per layer** field, specify the size of the filters for each layer of the element separated by a comma without spaces.

The default value of this parameter is `2,2,2`.

b. In the **Filters per layer** field, specify the number of filters for each layer of the ML model element separated by a comma without spaces.

The default value of this parameter is `50,50,50`.

c. In the **MaxPooling window size per layer** field, specify the maximum sampling window size values separated by a comma without spaces.

The default value of this parameter is `2,2,2`.

d. In the **Number of neurons in decoder** field, specify the number of neurons on the layers of the decoder.

14. If you have selected a neural network element with a TCN architecture, do the following:

a. In the **Regularization** field, specify the regularization coefficient in decimal format to prevent overfitting of the ML model element.

The default value of this parameter is `0.1`.

b. In the **Size of filters** field, specify the sizes of the filters for the ML model element.

The default value of this parameter is `2`.

   c. In the **Dilation per layer** field, specify the exponential expansion values of the output data on the layers separated by a comma without spaces.

      The default value of this parameter is `1,2,4`.

   d. In the **Activation function** drop-down list, select one of the following activation functions:

      - **linear**: A linear activation function whose result is proportional to the input value.
      - **relu**: A non-linear activation function that converts an input value to a value between zero and positive infinity. If the input value is less than or equal to zero, the function returns a value of zero; otherwise, the function returns the input value.

      The default value of this parameter is **linear**.

   e. In the **Number of stacks of residual blocks** field, specify the number of encoders.

      The default value of this parameter is `1`.

   f. In the **Decoder layer type** field, select one of the following types of layer to precede the output layer:

      - **TimeDistributedDense** (default): A fully connected architecture layer.
      - **GRU**: A layer with a recurrent architecture.

15. If you have selected a neural network element with a transformer architecture, do the following:

    a. In the **Encoder regularization** field, specify the regularization coefficient in the encoder in decimal format.

       The default value of this parameter is `0.01`.

    b. In the **Number of attention heads** field, specify the number of attention heads.

       The default value of this parameter is `1`.

    c. In the **Number of encoders** field, specify the number of encoders.

       The default value of this parameter is `1`.

    d. In the **Multipliers for calculating number of neurons per layer** field, provide the factors, separated by a comma without spaces, by which to multiply the number of input tags to calculate the number of neurons in the decoding layers.

16. In the upper-right corner of the window, click the **Save** button.

Adding an ML model element based on a diagnostic rule

System administrators and users who have the **Create models** permission from the Manage ML models group of rights can add ML model elements.

To add an ML model element based on a diagnostic rule:

1. In the main menu, select the **Models** section.

2. In the asset tree, next to the **Rules** group within an ML model to which you want to add a diagnostic rule, open the vertical menu **...** and select **Create element**.

   A list of options appears on the right.

3. In the **Name** field, specify a name for the diagnostic rule.

4. In the **Description** field, specify the diagnostic rule description.

5. In the **General element settings** settings block, do the following:

   a. In the **Reminder period (sec)** field, specify the period in seconds, upon reaching which the ML model will generate a repeated incident if anomalous behavior is retained in each UTG node.

      The default value of this setting is `0`, which corresponds to no reminders.

   b. In the **Period of recurring alert suppression (sec)** field, specify the period in seconds during which the ML model does not log repeated incidents for the same element.

      The default value of this setting is `0` (repeat incidents not suppressed).

   c. In the **Grid step (sec)** field, specify the element's UTG period in seconds expressed as a decimal.

   d. In the **Incident status** drop-down list, select a status to be automatically assigned to incidents logged by the ML model element.

   e. In the **Incident cause** drop-down list, select the cause to be automatically set for incidents logged by the ML model element.

   f. In the **Color of incident dot indicators** field, select the color of the indicator points of the incidents logged by the ML model element on the graphs in the **Monitoring** and **History** sections.

   g. In the **Expert opinion** field, specify the expert opinion to be automatically created for incidents logged by the ML model element.

6. If necessary, use the toggle switch to turn on the **Treat inconclusive result as positive** option.

   If Kaspersky MLAD cannot unequivocally evaluate the fulfillment of criteria specified in the **Time filter** and **Tag conditions** settings blocks, for example, due to the absence of observations for tags, the application will consider a rule to be triggered when this option is enabled.

7. In the **Time filter** settings block, do the following:

   a. Click the **Add interval** button.

   b. In the **Interval type** drop-down list, select one of the following time interval types:

      - **Fixed**. If you select this type of interval, specify the days of the week and the time interval during which the input data must be validated according to the specified criteria.

        You can specify only the beginning or the end of a single interval.

      - **Recurrent**. If you select this type of interval, specify the years, dates, days of the week, and daily time interval for periodically validating input data according to the specified criteria.

   c. If you want to add one more interval, click the **Add interval** button and complete step 7b.

   d. If you want to delete an interval, move the mouse cursor over the row with the required interval and click the **Delete interval** (✕) icon.

You can add one or more time intervals. If no time interval is specified, the diagnostic rule is applied in each UTG node.

8. To add tag behavior criteria, do the following:

   a. In the **Tag conditions** settings block, click the **Condition** button.

   b. In the **Tag** drop-down list, select the tag for which to add a tag behavior criterion.

      If you want to exclude the selected criterion from the condition block that you are adding, click **NOT** to the left of the selected tag. The **NOT** caption in the button will be highlighted in bold.

      For example, click **NOT** to add a condition that contains no steps with the specified settings.

   c. In the **Behavior** drop-down list, select one of the following tag behaviors that must be tracked:

      - **Over**: the tag value exceeds the specified threshold.
      - **Below**: the tag value falls below the specified threshold.
      - **Rising**: the trendline of tag values is increasing.
      - **Falling**: the trendline of tag values is decreasing.
      - **Level**: there are no pronounced changes in the trendline of tag values.
      - **Step change**: the trendline of the selected tag is displaying abrupt upward or downward shifts.
      - **Flat**: the selected tag is transmitting the same value.
      - **Spread**: abrupt changes in the spread of values are being observed around the trendline of the selected tag.

   d. In the **Window** field, specify the number of UTG steps.

   e. Depending on the value selected for **Behavior**, do one of the following:

      - If you selected **Over** or **Below**, use the **Threshold** field to specify the tag threshold value, and specify the minimum number of times the threshold value can be breached in a separate window in the **Minimum violations** field.
      - If you selected **Rising**, **Falling**, or **Level**, use the **Threshold slope** field to specify the trend slope percentage value that must be exceeded for the trend to be considered as growing or falling, and specify the time interval between adjacent trend estimates in the **Evaluation period** field.

        By default, the **Threshold slope** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine the trend direction automatically.

        By default, the **Evaluation period** setting has a value of `1`. With this value, the trend is estimated at each UTG node.
      - If you selected **Step change**, use the **Minimum change** field to specify the minimum shift value for the tag trendline, and select one of the following tag value change directions from the **Direction** drop-down list: **Any**, **Up** or **Down**.

        By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.
      - If you selected **Flat**, use the **Value** field to specify the value that the tag should transmit, and specify the maximum tag value spread in the **Spread** field.

By default, the **Value** setting is not defined. If the setting is not defined, any repeating tag value triggers the criterion.

- If you selected **Spread**, use the **Minimum change** field to specify the minimum value by which the tag value spread around the trendline can change, and select one of the following spread change directions in the **Direction** drop-down list: **Any**, **Flare**, or **Shrink**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

  The tag behavior criterion is met when the tag spread around the trendline increases and/or decreases.

f. To add a tag behavior criterion to a condition block, click the plus sign at the bottom of the condition block and repeat steps 8b through 8e.

g. If the block contains more than one tag behavior criterion, select one of the following logical operators between the criterion rows:

- **AND** if you need to track both criteria while a diagnostic rule is active.

- **OR** if you need to track one of the defined criteria while a diagnostic rule is active.

9. If you need to check whether the fulfillment of a pre-condition caused the fulfillment of a post-condition in a future UTG node, add a temporal operator:

a. In the **Tag conditions** settings block, click the **Wait** button.

The **Wait** button is available after at least one condition has been added.

A *precondition* is a block of conditions preceding the temporal operator. A *postcondition* is a block of conditions following a temporal operator.

The precondition block is checked in the current UTG node.

b. In the **Recess (steps)** field, specify the following time intervals:

- **from**: the interval between the current UTG node and the first future UTG node, in which the post-condition block is checked (minimum waiting interval).

- **to**: the interval between the current UTG node and the last future UTG node, in which the post-condition block is checked (maximum waiting interval).

The post-condition block is checked in the UTG nodes between the minimum and maximum waiting intervals.

c. In the **Check** drop-down list, select one of the following group operators:

- To check the fulfillment of tag behavior criteria from the post-conditions block in all UTG nodes between the minimum and maximum waiting intervals, select the **All steps** group operator.

- To check the fulfillment of tag behavior criteria from the post-conditions block in at least one UTG node between the minimum and maximum waiting intervals, select the **Any step** group operator.

The criteria check result is determined in the last node of the maximum waiting interval. If the check of the precondition block in the current UTG node gave a negative result (FALSE) or an undefined result (UNDEFINED), the same value will be the result of the check of the post-condition block.

If the check of the precondition block in the current UTG node gave a positive result (TRUE), then the check of the post-condition block is performed in each UTG node between the minimum and maximum waiting interval. The result of the check is determined by the fulfillment of the condition depending on the selected group operator: **All steps** or **Any step**.

If more than one condition check is performed using the temporal operator, then the result of the check of the previous temporal condition is a precondition for each subsequent check of the temporal condition.

10. Select one of the following logical operators between rule blocks:
    - **AND** if you need to track tag behavior criteria in both blocks while a diagnostic rule is active.
    - **OR** if you need to track tag behavior criteria in one of the blocks while a diagnostic rule is active.
11. In the upper-right corner of the window, click the **Save** button.

The new ML model element will be displayed in the **Rules** group within the selected ML model in the asset tree.

If an ML model contains only elements based on diagnostic rules, the model is assigned the *Trained* status. You can start inference for such an ML model. If the ML model contains untrained neural network elements, they must be trained before starting inference.

Changing an ML model element based on a diagnostic rule

You can change the settings of an ML model element based on a diagnostic rule.

System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can edit elements of ML models.

To change an element of an ML model based on a diagnostic rule:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the element based on a diagnostic rule that you want to edit.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the **Edit** button.
4. In the **Name** field, specify a new name for the diagnostic rule.
5. In the **Description** field, specify a new description for the diagnostic rule.
6. If necessary, in the **General element settings** settings block, do the following:

   a. In the **Reminder period (sec)** field, specify the period in seconds, upon reaching which the ML model will generate a repeated incident if anomalous behavior is retained in each UTG node.

   The default value of this setting is `0`, which corresponds to no reminders.

   b. In the **Period of recurring alert suppression (sec)** field, specify the period in seconds during which the ML model does not log repeated incidents for the same element.

   The default value of this setting is `0` (repeat incidents not suppressed).

   c. In the **Grid step (sec)** field, specify the UTG period for the element in seconds.

   d. In the **Incident status** drop-down list, select a status to be automatically assigned to incidents logged by the ML model element.

    e. In the **Incident cause** drop-down list, select the cause to be automatically set for incidents logged by the ML model element.

    f. In the **Color of incident dot indicators** field, select the color of the indicator points of the incidents logged by the ML model element on the graphs in the **Monitoring** and **History** sections.

    g. In the **Expert opinion** field, specify the expert opinion to be automatically created for incidents logged by the ML model element.

7. If necessary, use the toggle switch to turn on the **Treat inconclusive result as positive** option.

   If Kaspersky MLAD cannot unequivocally evaluate the fulfillment of criteria specified in the **Time filter** and **Tag conditions** settings blocks, for example, due to the absence of observations for tags, the application will consider a rule to be triggered when this option is enabled.

8. If necessary, do the following in the **Time filter** settings block:

   a. In the **Interval type** drop-down list, select one of the following time interval types:

   - **Fixed**. If you select this type of interval, specify the days of the week and the time interval during which the input data must be validated according to the specified criteria.

     You can specify only the beginning or the end of a single interval.

   - **Recurrent**. If you select this type of interval, specify the years, dates, days of the week, and daily time interval for periodically validating input data according to the specified criteria.

   b. If you want to add one more interval, click the **Add interval** button and complete step 8a.

   c. If you want to delete an interval, move the mouse cursor over the row with the required interval and click the **Delete interval** (×) icon.

   You can add one or more time intervals. If no time interval is specified, the diagnostic rule is applied in each UTG node.

9. To edit a tag behavior condition, do the following:

   a. In the **Tag** drop-down list, select the tag for which to add a tag behavior criterion.

   If you want to exclude the selected criterion from the condition block that you are adding, click **NOT** to the left of the selected tag. The **NOT** caption in the button will be highlighted in bold.

   For example, click **NOT** to add a condition that contains no steps with the specified settings.

   b. In the **Behavior** drop-down list, select one of the following tag behaviors that must be tracked:

   - **Over**: the tag value exceeds the specified threshold.

   - **Below**: the tag value falls below the specified threshold.

   - **Rising**: the trendline of tag values is increasing.

   - **Falling**: the trendline of tag values is decreasing.

   - **Level**: there are no pronounced changes in the trendline of tag values.

   - **Step change**: the trendline of the selected tag is displaying abrupt upward or downward shifts.

   - **Flat**: the selected tag is transmitting the same value.

- **Spread**: abrupt changes in the spread of values are being observed around the trendline of the selected tag.

c. In the **Window** field, specify the number of UTG steps.

d. Depending on the value selected for **Behavior**, do one of the following:

- If you selected **Over** or **Below**, use the **Threshold** field to specify the tag threshold value, and specify the minimum number of times the threshold value can be breached in a separate window in the **Minimum violations** field.

- If you selected **Rising**, **Falling**, or **Level**, use the **Threshold slope** field to specify the trend slope percentage value that must be exceeded for the trend to be considered as growing or falling, and specify the time interval between adjacent trend estimates in the **Evaluation period** field.

  By default, the **Threshold slope** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine the trend direction automatically.

  By default, the **Evaluation period** setting has a value of `1`. With this value, the trend is estimated at each UTG node.

- If you selected **Step change**, use the **Minimum change** field to specify the minimum shift value for the tag trendline, and select one of the following tag value change directions from the **Direction** drop-down list: **Any**, **Up** or **Down**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

- If you selected **Flat**, use the **Value** field to specify the value that the tag should transmit, and specify the maximum tag value spread in the **Spread** field.

  By default, the **Value** setting is not defined. If the setting is not defined, any repeating tag value triggers the criterion.

- If you selected **Spread**, use the **Minimum change** field to specify the minimum value by which the tag value spread around the trendline can change, and select one of the following spread change directions in the **Direction** drop-down list: **Any**, **Flare**, or **Shrink**.

  By default, the **Minimum change** setting is not defined. If the setting is not defined, Kaspersky MLAD will determine it automatically.

  The tag behavior criterion is met when the tag spread around the trendline increases and/or decreases.

e. To add a tag behavior criterion to a condition block, click the plus sign at the bottom of the condition block and repeat steps 9a through 9d.

f. If the block contains more than one tag behavior criterion, select one of the following logical operators between the criterion rows:

- **AND** if you need to track both criteria while a diagnostic rule is active.

- **OR** if you need to track one of the defined criteria while a diagnostic rule is active.

10. If you need to edit the temporal operator:

a. In the **Recess (steps)** field, specify the following time intervals:

- **from**: the interval between the current UTG node and the first future UTG node, in which the post-condition block is checked (minimum waiting interval).

- **to**: the interval between the current UTG node and the last future UTG node, in which the post-condition block is checked (maximum waiting interval).

The post-condition block is checked in the UTG nodes between the minimum and maximum waiting intervals.

b. In the **Check** drop-down list, select one of the following group operators:

- To check the fulfillment of tag behavior criteria from the post-conditions block in all UTG nodes between the minimum and maximum waiting intervals, select the **All steps** group operator.
- To check the fulfillment of tag behavior criteria from the post-conditions block in at least one UTG node between the minimum and maximum waiting intervals, select the **Any step** group operator.

The criteria check result is determined in the last node of the maximum waiting interval. If the check of the precondition block in the current UTG node gave a negative result (FALSE) or an undefined result (UNDEFINED), the same value will be the result of the check of the post-condition block.

If the check of the precondition block in the current UTG node gave a positive result (TRUE), then the check of the post-condition block is performed in each UTG node between the minimum and maximum waiting interval. The result of the check is determined by the fulfillment of the condition depending on the selected group operator: **All steps** or **Any step**.

If more than one condition check is performed using the temporal operator, then the result of the check of the previous temporal condition is a precondition for each subsequent check of the temporal condition.

11. Select one of the following logical operators between rule blocks:
    - **AND** if you need to track tag behavior criteria in both blocks while a diagnostic rule is active.
    - **OR** if you need to track tag behavior criteria in one of the blocks while a diagnostic rule is active.
12. In the upper-right corner of the window, click the **Save** button.

Removing an ML model element

When removing an ML model element, Kaspersky MLAD also deletes the results of the work of the selected element of the ML model.

System administrators and users who have the **Remove models** permission from the Manage ML models group of rights can remove elements of ML models.

To remove an ML model element:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model element that you want to delete.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the trash bin icon (🗑).
4. In the window that opens, confirm the deletion of the ML model element.

Cloning an ML model

System administrators and users who have the **Copy models** permission from the **Manage ML models** group of rights can clone ML models.

You can create an ML model by cloning a previously added ML model. When cloning, a new ML model is created. The new ML model contains the same elements, parameters of the ML model and its elements, as well as the training state of the neural network elements as the ones of the ML model being cloned at the time of its cloning.

When cloning an ML model that was created manually or from a template based on a manually created ML model, you can add neural network elements and/or the elements based on diagnostic rules to the cloned ML model, as well as modify or delete them.

When cloning an ML model that was imported into the application or created using a template based on an imported ML model, you cannot change the set of elements of the cloned ML model.

Before running inference, you can change the training settings and retrain the neural network elements of the copied ML model. You can also start inference after the ML model has been published.

To clone an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model that you want to copy.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the **Copy model** (⧉) icon.

   The **Model copying** pane appears on the right.
4. In the **Name** field, specify the ML model name.

   The ML model name must not be longer than 100 characters.

   By default, an ML model is assigned a name in the following format: `< name of the original ML model>_Cloned_ <date and time of cloning>`.
5. In the **Asset** drop-down list, select the asset to which you want to assign the new ML model.
6. Click the **Save** button.

The new ML model displays in the **Models** group of the asset tree. The **Models** group is created automatically and displayed as part of the selected section of the asset tree. The **Models** group contains the **Neural networks** and **Rules** subgroups for storing ML model elements based on neural networks and diagnostic rules.

Working with ML model templates

This section provides instructions on working with ML model templates.

You can create a template of an existing ML model to reuse its algorithm structure, set of elements, and training state at the time of the template creation. You can use a created template to add new ML models.

If the original ML model used as a template was created manually, you can add neural network elements and/or elements based on diagnostic rules to the ML model created based on such template, as well as modify or delete them.

If the original ML model used to create a template was imported to Kaspersky MLAD, the set of elements of the ML model created based on such a template cannot be changed.

Before inference, the ML model needs to train all its neural network elements. You can also start inference if the ML model has been published.

Creating a template based on an ML model

System administrators and users who have the **Create model templates** permission from the **Manage ML models** group of rights can create templates based on ML models.

You can create an ML model template based on a previously added ML model. The created templates retain the algorithm structure, set of elements, tag composition, and the training state of the source ML model.

You can create a template based on a previously added ML model if this ML model includes a neural network element for which input and output tags are defined, and/or an element based on a diagnostic rule for which rule conditions have been created.

To create a template based on an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the name of the ML model based on which you want to create a template, open the vertical menu **...** and select **Create template**.

   A list of options appears on the right.
3. Enter the template name in the **Name** field.

   You can enter up to 100 characters.

   By default, a template is assigned a name in the format `Template_<ML model name>_<date and time of template creation>`.
4. To change the names of the template tags, in the **Template tag name** column specify the new names for the relevant tags.

   If the tags used in the ML model you are using to create the template were loaded or created in the **Assets** section of the administrator menu, their names are automatically assigned to the tags in the template. If a tag used in the ML model was not detected in Kaspersky MLAD, this tag will be assigned the default name in the format **Tag <Model tag ID>**.

   You can specify a template tag name different from the tag names in the **Assets** section of the administrator menu. Template tags and tags in the **Assets** section are mapped based on the IDs of the ML model tags, which you can specify when creating an ML model from a template.
5. Click the **Save** button.

The new ML model template appears in the **Templates** group of the asset tree. The **Templates** group is created automatically and displayed as part of the selected section of the asset tree.

Editing an ML model template

You can edit the settings of a created ML model template.

System administrators and users who have the **Edit model templates** permission from the **Manage ML models** group of rights can edit ML model templates.

To edit an ML model template:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the template that you want to edit.

   A list of options appears on the right.
3. In the upper-right corner of the window, click the **Edit** button.
4. In the **Name** field, enter the new template name.

   You can enter up to 100 characters.

   By default, a template is assigned a name in the format `Template_<ML model name>_<date and time of template creation>`.
5. To change the names of the template tags, in the **Template tag name** column specify the new names for the relevant tags.

   You can specify a template tag name different from the tag names in the **Assets** section of the administrator menu. Template tags and tags in the **Assets** section are mapped based on the IDs of the ML model tags, which you can specify when creating an ML model from a template.
6. Click the **Save** button.

Creating an ML model based on a template

System administrators and users who have the **Create models** permission from the **Manage ML models** group of rights can create ML models based on templates.

You can create a new ML model based on available templates. When creating an ML model, you can specify the IDs of tags that should be used in the new ML model.

To create an ML model based on a template:

1. In the main menu, select the **Models** section.
2. In the asset tree, next to the name of the template that you want to use to create an ML model, open the vertical menu **...** and select **Create model**.

   The **Creating a model** pane opens on the right.
3. Enter a name for the new ML model in the **Model name** field.

The ML model name must not be longer than 100 characters.

4. In the **Model tag name** column, select the tag names for each tag of the created ML model.

   Template tags and tags in the **Assets** section in the administrator menu are mapped based on the names of the ML model tags.

5. Click the **Save** button.

The new ML model displays in the **Models** group of the asset tree. The **Models** group is created automatically and displayed as part of the selected section of the asset tree. The **Models** group contains the **Neural networks** and **Rules** subgroups for storing ML model elements based on neural networks and diagnostic rules.

The state of the created ML model will match the training state of the source ML model when the template was created.

Removing an ML model template

> System administrators and users who have the **Delete model templates** permission from the **Manage ML models** group of rights can remove ML model templates.

You can remove an ML model template from Kaspersky MLAD. Deleting a template does not remove ML models based on this template.

To remove an ML model template:

1. In the main menu, select the **Models** section.

2. In the asset tree, select the ML model template that you want to delete.

   A list of options appears on the right.

3. In the upper-right corner of the window, click the trash bin icon (🗑).

4. Confirm deletion of the ML model template.

The selected ML model template will be removed from Kaspersky MLAD.

Changing the parameters of an ML model

You can change the settings of an ML model that was created manually, imported into Kaspersky MLAD, created from a template, or copied.

> System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can edit the settings of ML model elements.

To change the parameters of an ML model:

1. In the main menu, select the **Models** section.

2. In the asset tree, select the ML model whose settings you want to edit

A list of options appears on the right.

3. In the upper-right corner of the window, click the **Edit** button.

4. In the **Name** field, specify the ML model name.

   The ML model name must not be longer than 100 characters.

5. In the **Description** field, specify the ML model description.

6. If the ML model was not imported into the application or was created on the basis of an imported ML model, in the **Inference indicator** settings block, select the markups for conducting inference.

7. To view the data selected by the markups, click **On graph**.

   Markups are displayed in the colors selected when they were created.

8. In the upper-right corner of the window, click the **Save** button.

Training a neural network element of an ML model

With Kaspersky MLAD, you can train a neural network element for an ML model that was created manually, imported into Kaspersky MLAD, created from a template, or copied.

> System administrators and users who have the **Train models** permission from the **Manage ML models** group of rights can train elements of ML models.

To train an ML model element:

1. In the main menu, select the **Models** section.

2. In the asset tree, select the neural network element that you want to train.

   A list of options appears on the right.

3. Open the **Training** tab and click the **Edit** button in the upper-right corner of the window.

4. In the **Data selection interval** field, specify the data time interval on which you want to train the ML model.

5. To apply markups when selecting data for training the ML model within a selected interval, select one or several markups in the **Markups** field.

   The selected markups will form a learning indicator.

6. To view the data that will be selected by the markups, click **On graph**.

   Markups are displayed in the colors that were specified when they were created.

7. If necessary, enable **Advanced training settings** and do the following:

   a. In the **Maximum training duration (sec)** field, specify a maximum time in seconds that the Kaspersky MLAD server can spend for training an ML model.

   b. In the **Validation split** field, use a decimal value to specify the share of the validation sample as a percentage of the entire dataset used to train the ML model.

You can specify a value in the range of `0` to `1`.

The default value of this parameter is `0.2`.

c. In the **Maximum epoch count** field, specify the maximum number of epochs for training the ML model.

   The default value of this parameter is `500`.

d. In the **Patience** field, specify the number of epochs with no improvement in training quality to wait before stopping the ML model training process early.

   Stopping the ML model training early avoids overfitting of the model. Training in this case is considered to be completed successfully.

   The default value of this parameter is `15`.

e. In the **Resolution of training results graphs** field, use a decimal value to specify the graph resolution for displaying training results on the **Training results** tab.

   You can specify a value in the range of `0` to `1`.

f. In the **Batch size** field, specify the number of selection items that must be sent for training within the iteration.

   The default value of this parameter is `16`.

g. In the **Block count** field, specify the number of blocks into which you want to split the dataset for training the ML model.

   The default value of this parameter is `4`.

h. In the **Inference mode** drop-down list, select one of the following values:

   - If you want to load all batches into RAM, select **Fast inference**.

     This inference mode allows you to perform inference faster.

   - If you want to load data batches into RAM one at a time, select **Memory saving mode**.

     This inference mode allows inference to be performed with minimal expenditure of RAM, but it will take place slower than in **Fast inference** mode.

   The selected inference mode is applied only while training a neural network element of an ML model.

i. In the **Training mode** drop-down list, select one of the following values:

   - If you want to load the entire dataset for training the model into RAM, select **Load whole dataset to RAM**.

   - If you want to load one data block at a time into RAM and generate validation blocks from the end of the dataset, select **Validate at the end of the dataset**.

   - If you want to load one data block at a time into RAM without generating validation blocks, select **Run validation in each training data block**.

     Validation data is generated from each training data block.

j. In the **Memory allocation mode** drop-down list, select one of the following settings:

   - **Reserve minimum amount of free RAM**. If this setting is selected, the Trainer service will make sure that the minimum amount of memory specified in the **Amount of RAM, MB** field remains free when training the ML model.

- **Reserve maximum available amount of RAM for model training**. If this setting is selected, the Trainer service will use the maximum amount of RAM specified in the **Amount of RAM, MB** field when training the ML model.

k. To consider previous training results while training an ML model on new data, enable the option to **Initialize model weights with values from previous training results**.

l. If you want to shuffle the data to improve the quality of ML model training, enable the **Shuffle data** option.

8. In the upper-right corner of the window, click the **Save** button.

9. In the information block located above the training settings, click the **Train element** button.

The information block will show the number of the current training epoch of the ML model element. After the training is complete, you can view the training results of an ML model element in the **Training results** tab.

After training all the neural network elements within an ML model, the model is assigned the *Trained* status. If required, you can retrain the ML model element by clicking **Restart training**.

Viewing the training results of an ML model element

You can view the results of training the neural network elements of an ML model.

System administrators and users who have the **Train models** permission from the **Manage ML models** group of rights can view the results of training ML model elements.

To view the training results of an ML model element:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model element whose training result you want to view.

   A panel with the settings of the selected element will appear on the right.
3. Select the **Training results** tab.

If the ML model element has been successfully trained, the following information about the training results is displayed in the **Training results** tab:

- Message about successful completion of training of an ML model element.

  If you want to view the training settings for an element that were specified during its creation, click the **Training settings** link.
- **User**: The name of the user who started training the ML model element.
- **Training interval**: The time spent by the Kaspersky MLAD server for training the ML model element.
- **Start of training**: The date and time when the Trainer service began training the ML model element.
- **End of training**: The date and time that training of the ML model element finished. ML model element weights have been updated by the Trainer service.
- **Total training duration**: The duration of data time intervals considering the markups in the training dataset.

- **Number of UTG nodes**: The number of UTG nodes included in the training set.
- **Training and validation errors**: A graph showing the training and validation errors for each training epoch.
- **Model prediction**: Graphs showing model predictions for the output tags and the overall prediction error.

Preparing an ML model for publication

After training the ML model, you can prepare it for publication. An ML model ready for publishing cannot be modified.

> System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can prepare an ML model for publication.

To prepare an ML model for publication:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model you want to prepare for publication.

   A list of options appears on the right.
3. Click the **Prepare to publish** button.

   The ML model is assigned the *Ready for publication* status. Notify the officer responsible for publishing the ML model that it is ready, or, if you have the required permissions, publish the ML model.

To make changes to the ML model before publishing, click the **Back to edit mode** button. The ML model will revert to a status of *Trained*.

Publishing an ML model

You can publish an ML model for logging incidents based on the operational data from the monitored asset.

> System administrators and users who have the **Edit model drafts** permission from the **Manage ML models** group of rights can publish ML models.

To publish an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model that you want to publish.

   A list of options appears on the right.
3. Click **Publish**.

   The ML model is assigned the *Published* status.

When the inference is started, the ML model will log incidents.

Starting and stopping ML model inference

You can start or stop the inference of an ML model with a status of *Trained* or *Published* on historical or newly received telemetry data.

To start the ML model inference:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model whose inference you want to run.

   A list of options appears on the right.
3. Select the **Inference** tab.
4. In the **Inference type** drop-down list, select one of the following values:
   - **Historical** to run ML model inference on historical telemetry data. If you select this value, specify the data time interval for running the ML model.
   - **Real-time** to run ML model inference on telemetry data that is being received in real time.
5. Click the **Start** button.

If historical inference was started, Kaspersky MLAD will add the ML model to the inference queue.

To stop the ML model inference:

1. In the main menu, select the **Models** section.
2. In the asset tree, select the ML model whose inference you want to stop.

   A list of options appears on the right.
3. Select the **Inference** tab.
4. Click the **Stop** button.

Kaspersky MLAD will stop inference for the selected ML model.

Viewing the data flow graph of an ML model

You can view the data flow graph in ML models.

To view the data flow graph in an ML model:

1. In the main menu, select the **Models** section.
2. In the asset tree, select a neural network element, the data flow graph that you want to view.

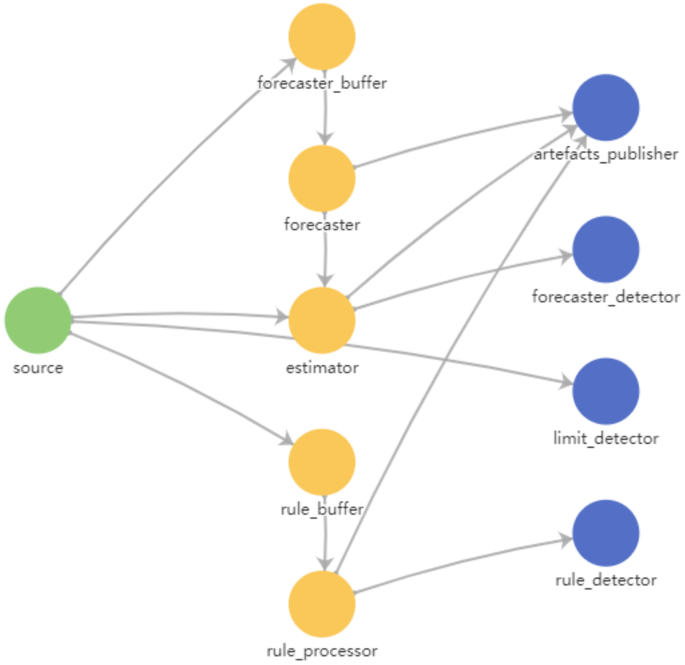
   A list of options appears on the right.

3. Select the **Data flow graph** tab.

   The ML model data flow graph is displayed on the right.

4. If you need to view the settings of an ML model, move the mouse cursor over it.

   A window listing the values of settings of the selected element will be displayed.



ML model data flow graph

Removing an ML model

You can remove one or more ML models from Kaspersky MLAD.

After the ML model is removed, its artifacts, such as predictions, individual errors, prediction errors, or rule progress indicators, as well as incidents registered by the ML model, will be deleted.

System administrators and users who have the **Remove models** permission from the **Manage ML models** group of rights can remove ML models.

To remove an ML model:

1. In the main menu, select the **Models** section.

2. In the asset tree, select the ML model to be deleted.

   A list of options appears on the right.

3. In the upper-right corner of the window, click the trash bin icon (🗑).

4. Confirm deletion of the ML model.

The selected ML model will be removed from Kaspersky MLAD.

Managing presets

A *preset* is a set of tags generated by a user in arbitrary order or created automatically when an incident is registered. A set of tags in a custom preset can correspond to a certain aspect of the technological process or a section of the monitored asset.

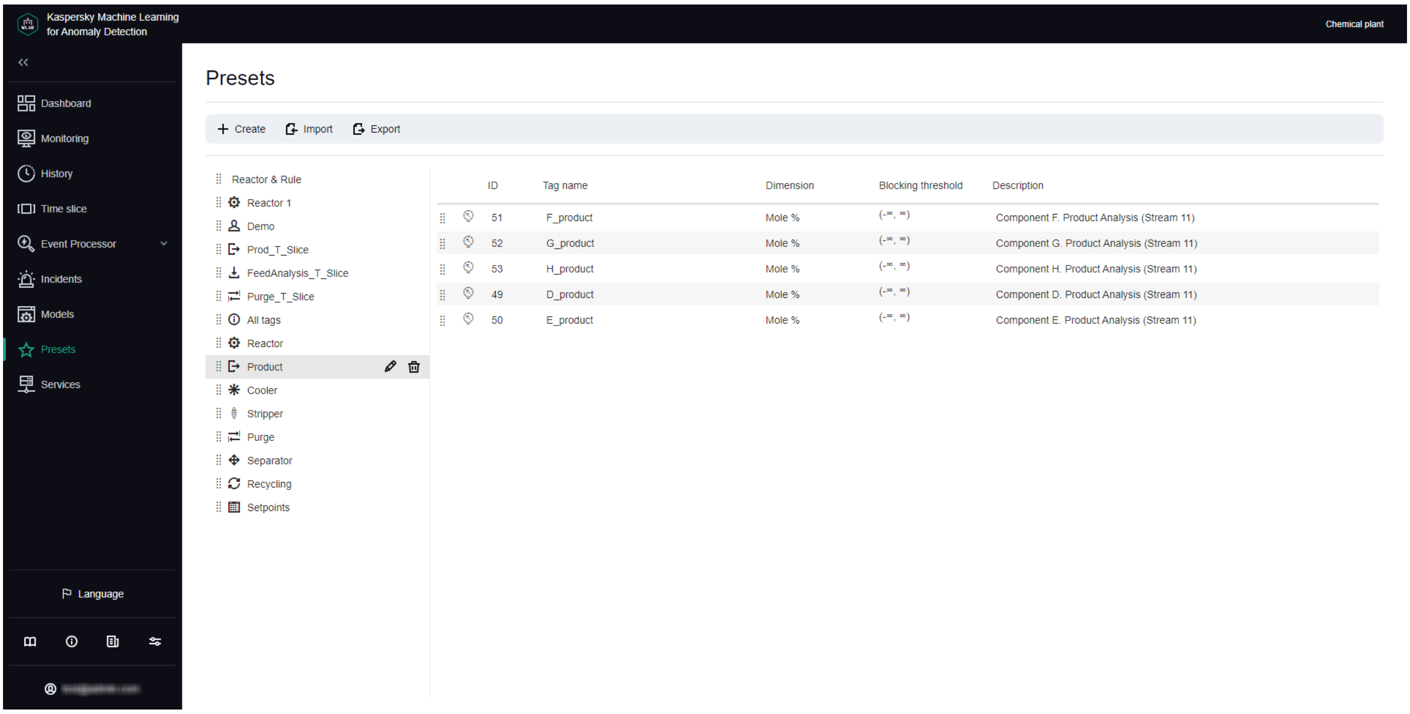
In the **Presets** section, the left side of the window displays a list of available custom presets, and the right side of the window shows a list of tags included in the selected preset.

To view the received data on the graphs in the **History** and **Monitoring** sections, upload the preset configuration to Kaspersky MLAD from a JSON file. As part of Kaspersky MLAD deployment, a common preset configuration can be created for all users.

In the **Presets** section, you can also do the following:

- Create necessary presets that include tags corresponding to the industrial units of the monitored asset. The presets created by you are displayed only for your user account.
- Edit presets (add, group, or delete tags).
- Delete presets.
- Export presets to a JSON file.

You can also specify expressions with simple arithmetic operations (such as addition, subtraction, multiplication, and division) to calculate derived tag values.



[redacted]

ID	Tag name	Dimension	Blocking threshold	Description
51	F_product	Mole %	(-∞, ∞)	Component F. Product Analysis (Stream 11)
52	G_product	Mole %	(-∞, ∞)	Component G. Product Analysis (Stream 11)
53	H_product	Mole %	(-∞, ∞)	Component H. Product Analysis (Stream 11)
49	D_product	Mole %	(-∞, ∞)	Component D. Product Analysis (Stream 11)
50	E_product	Mole %	(-∞, ∞)	Component E. Product Analysis (Stream 11)

Presets section

Viewing a preset

You can view presets you created or uploaded to Kaspersky MLAD for your monitored asset.

To view a preset:

1. In the main menu, select the **Presets** section.

   The list of presets is displayed in the left part of the workspace.

2. Click the relevant preset.

   The table on the right shows the tags that are included in the selected preset. The following information is displayed for each tag included in the preset:

   - **ID** refers to the tag ID.
   - **Tag name** refers to the tag name.
   - **Dimension** refers to the tag measurement units.
   - **Blocking threshold** refers to the blocking thresholds; when these thresholds are reached, incidents are registered if the Limit Detector is enabled.
   - **Description** refers to a description of the tag.

If necessary, you can change the preset or create a new preset.

Creating a new preset

You can create new presets in Kaspersky MLAD.

When creating a preset, you can specify an expression to use for calculating the values of tags in the preset to display these values on the graph in the **Time slice** section. For example, you can use the specified expressions to view personal tag errors, predicted tag values, and the values of tags received from the monitored asset's sensors at the same time. You can use the following variables in your expressions:

- *$tagValue* is the received tag value (based on the results of monitoring).
- *$tagError* is the personal tag error.
- *$tagPrediction* is the predicted tag value.
- *$tagX* is the X coordinate of the monitored asset's sensor location specified when creating the tag.
- *$tagY* is the Y coordinate of the monitored asset's sensor location specified when creating the tag.
- *$tagZ* is the Z coordinate of the monitored asset's sensor location specified when creating the tag.

To create a new preset:

1. In the main menu, select the **Presets** section and click the **Create** button.

   The **Create preset** window opens.

2. Specify the name of the preset in the **Preset name** field.

3. If necessary, click the **Choose icon** button and select an icon for the preset in the opened window.

By default, the preset is assigned a sun icon (☼).

You can upload a preset icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

If you want to delete the preset icon, click the preset icon and then click **Delete** in the opened window.

4. If you want to add an expression for calculating tag values to display them on a graph in the **Time slice** section, do the following:

   a. Turn on the **Configure expressions for Time slice** toggle switch.

   b. In the **X-axis caption** field, enter the caption to be displayed on the x-axis.

   c. Click the **Add expression** button and specify the following values in the drop-down section:

   - In the **Expression name** field, enter the name of the expression.

   - In the **Y-axis caption** field, enter the caption to be displayed on the y-axis.

   - In the **Expression for calculation** field, enter an expression for calculating tag values.

     You can define expressions with simple arithmetic operations (such as addition, subtraction, multiplication, and division). For example, if the sensors are reporting temperature in Fahrenheit, you can use the following expression to display the temperature in Celsius:

     ```
     5/9 * ($tagValue - 32)
     ```

     If necessary, you can add multiple expressions for the **Time slice** section.

   - In the **Graph color** field, select the color of the graph that will be displayed for the preset in the **Time slice** section.

   d. If you want to delete an expression from a preset for the **Time slice** section, click the trash bin icon (🗑) in the lower-right corner of the expression section.

5. If you need to add tags that are part of another preset, select this preset from the **Copy tags from selected preset** drop-down list.

6. Add tags to the preset by selecting the check boxes next to the relevant tags in the asset tree below. You can search for tags by entering the tag name in the **Search by tag name** field.

7. If you need to delete tags from a preset, clear the check boxes next to the tags you want to delete in the asset tree.

8. Click the **Save** button.

The new preset is displayed in the **Presets** section in the list of presets on the left and in the drop-down list of presets in the **History** and **Monitoring** sections. The preset for which step 4 of these instructions was performed will also be displayed in the drop-down list of presets in the **Time slice** section.

If necessary, you can change the position of presets in the list of presets. To do this, drag the preset up or down in the list by the dots (⠿) to the left of its icon.

Editing a preset

You can edit the presets you created or uploaded.

To edit a preset:

1. In the main menu, select the **Presets** section.
2. On the opened page, select the relevant preset from the list of presets on the left.

   The table on the right shows all tags that are included in the selected preset.

   If necessary, change the position of the tags in the table. To do this, drag the desired tag up or down in the asset tree by the dots (⠿) to the left of its icon.
3. Click the **Change preset** (✎) button next to the selected preset.

   The **Edit preset** window opens.
4. If required, enter the new name of the preset in the **Preset name** field.

   You can also modify the preset name in the preset list. To do this, double-click the preset name, in the opened field enter a new preset name, and press `ENTER`.
5. If you need to change the preset icon, click the **Choose icon** button and select the appropriate icon in the opened window.

   You can upload a preset icon by clicking the **Load icon** button. Images of any format larger than 128x128 pixels are shrunk to 128x128 while maintaining the aspect ratio. The size of the uploaded image in SVG format must not exceed 200 KB.

   If you want to delete the preset icon, click the preset icon and then click **Delete** in the opened window.
6. If you want to add an expression for calculating tag values to display them on a graph in the **Time slice** section, do the following:

   a. Turn on the **Configure expressions for Time slice** toggle switch.

   b. In the **X-axis caption** field, enter the caption to be displayed on the x-axis.

   c. Click the **Add expression** button and specify the following values in the drop-down section:

   - In the **Expression name** field, enter the name of the expression.
   - In the **Y-axis caption** field, enter the caption to be displayed on the y-axis.
   - In the **Expression for calculation** field, enter an expression for calculating tag values.

     You can define expressions with simple arithmetic operations (such as addition, subtraction, multiplication, and division). For example, if the sensors are reporting temperature in Fahrenheit, you can use the following expression to display the temperature in Celsius:

     ```
     5/9 * ($tagValue - 32)
     ```

     If necessary, you can add multiple expressions for the **Time slice** section.
   - In the **Graph color** field, select the color of the graph that will be displayed for the preset in the **Time slice** section.

   d. To delete an expression from a preset for the **Time slice** section, click the trash bin icon (🗑) in the lower-right corner of the expression section.

7. If necessary, add tags to the preset by selecting the check boxes next to the relevant tags in the list of tags below. You can search for tags by entering the tag name in the **Search by tag name** field.

8. If necessary, clear the check boxes next to the names of the tags that you want to remove from the preset.

9. Click the **Save** button.

   The changed preset will be updated in the list of presets in the **Presets** section and in the drop-down list of presets in the **History** and **Monitoring** sections. The changed preset for which step 6 of these instructions was performed will also be displayed in the drop-down list of presets in the **Time slice** section.

   If necessary, you can change the position of presets in the list of presets. To do this, drag the preset up or down in the list by the dots (⠿) to the left of its icon.

Deleting a preset

You can delete the presets you created or uploaded.

To delete a preset:

1. In the main menu, select the **Presets** section.

2. On the opened page, select the relevant preset from the list of presets on the left.

3. Click the **Delete preset** (🗑) button next to the selected preset.

4. In the opened **Delete preset** window, click **Yes** to confirm deletion of the preset.

   The preset will be deleted from the list of presets.

Loading a preset configuration from a file

You can load a preset configuration to Kaspersky MLAD from a JSON file.

To upload a preset configuration to Kaspersky MLAD:

1. In the main menu, select the **Presets** section.

2. In the upper part of the opened page, click the **Import** button.

3. Select the JSON file containing the preset configuration on your local drive.

   The selected file will be loaded into Kaspersky MLAD, and new presets will be displayed in the list of presets.

Saving a preset configuration to a file

You can save the presets you created and uploaded to Kaspersky MLAD as a JSON file.

To save the presets you created and uploaded to Kaspersky MLAD to a file:

1. In the main menu, select the **Presets** section.

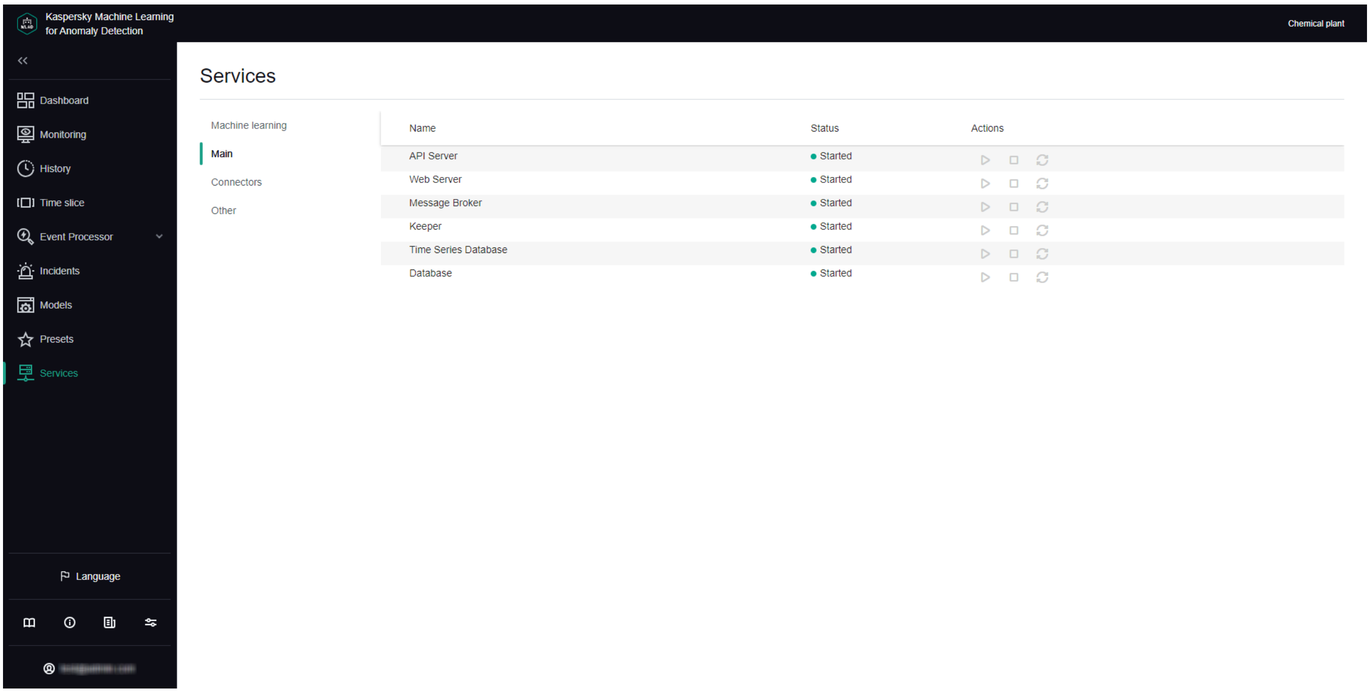
2. In the upper part of the opened page, click the **Export** button.

The presets you created and uploaded to Kaspersky MLAD will be saved to a JSON file on the local drive.

Managing services

The **Services** section displays a table containing information about services and their statuses. In the Kaspersky MLAD web interface, services are grouped by their functionality, and the following information is displayed for each service:

- **Name** is the name of the service.
- **Status** refers to the current status of the service (*Started*, *Stopped*, *Starting*, *Unavailable*).
- **Actions** are the available actions (start, stop, and restart).



Name	Status	Actions
API Server	● Started	▷ □ ⟳
Web Server	● Started	▷ □ ⟳
Message Broker	● Started	▷ □ ⟳
Keeper	● Started	▷ □ ⟳
Time Series Database	● Started	▷ □ ⟳
Database	● Started	▷ □ ⟳

Services section

Viewing the status of a service

You can view the status of a service to make sure that the service was successfully started or stopped.

> System administrators and users who have the **View statuses of application services** permission from the Working with application services group of rights can view the status of a service.

Kaspersky MLAD checks the statuses of services every 30 seconds.

To view the status of a service:

In the main menu, select the **Services** section.

The **Services** section opens to display a table listing all available services, their statuses, and available actions (start, stop, and restart).

Starting, stopping, and restarting services

Kaspersky MLAD lets you start, stop and restart services.

> System administrators and users who have the **Manage statuses of application services** permission from the **Working with application services** group of rights can start, stop, and restart services.

To start, stop, or restart a service:

1. In the main menu, select the **Services** section.
2. On the opened page, select one of the following subsections: **Machine learning**, **Main**, **Connectors** or **Other**.
3. Do one of the following for the relevant service:
   - To start a service, click **Start service** (▷).
   - To stop a service, click **Stop service** (□).
   - To restart a service, click **Restart service** (⟳).

   The new status of the service is displayed in the **Status** column.

Troubleshooting

This section describes possible problems in the operation of Kaspersky MLAD and methods for resolving them.

When connecting to Kaspersky MLAD, the browser displays a certificate warning

Problem

When attempting to connect to Kaspersky MLAD, the browser displays a warning that the security certificate or the established connection is not trusted. The contents of the warning depend on the specific browser being used.

Solution

After Kaspersky MLAD is installed, a self-signed certificate is used by default to connect to the web interface. When using a self-signed certificate, the browser displays a warning that the security certificate or the connection being established is not trusted. To use a trusted certificate, you need to contact a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator. An employee can update certificates for connecting to Kaspersky MLAD using the web interface.

You can temporarily use a self-signed certificate to connect to Kaspersky MLAD (for example, during test operation). When using a self-signed certificate, in the browser warning window select the option that lets you continue connecting. After connecting to Kaspersky MLAD, the browser window displays a warning about the certificate. The text of the message depends on the specific browser being used.

If the browser displays a warning after a trusted certificate is installed, then the certificate may have been spoofed by a malicious actor. Contact the Technical Support.

The hard drive has run out of free space

Problem

The hard drive of the computer on which Kaspersky MLAD is installed has run out of free disk space.

Solution

The computer must meet the hardware and software requirements to ensure proper functioning of the application.

To ensure that the application functions correctly:

On the hard drive of the computer, free up sufficient space to satisfy the minimum free disk space requirements.

The operating system restarted unexpectedly

Problem

Unexpected restart of a computer with Kaspersky MLAD installed.

Solution

Wait for the computer restart to finish. After the computer has restarted, the following statuses of Kaspersky MLAD are possible:

- Kaspersky MLAD has fully resumed normal operation.
- Kaspersky MLAD has not resumed normal operation.
  If the malfunction persists, please contact Kaspersky Technical Support.

Cannot connect to the Kaspersky MLAD web interface

Problem

When connecting to the web interface of Kaspersky MLAD after correct password is entered, the following error is displayed: *Error! Invalid server error.*

Solution

Often, the error *Error! Invalid server error* occurs because the server hosting Kaspersky MLAD has run out of free hard drive space.

To restore correct operation of the application:

On the hard drive of the server, free up sufficient space to satisfy the minimum free disk space requirements.

After freeing up disk space, if you still cannot connect to the web interface of Kaspersky MLAD, please contact Technical Support.

Graphs are not displayed in the History and Monitoring sections

Problem

The **History** and **Monitoring** sections are not showing graphs.

This may be caused by the following:

- Presets were not imported into Kaspersky MLAD.
- The selected preset contains no tags.
- Time interval with no data is selected in the **History** section.

- The connector used to receive data from the monitored asset is not running.
- The monitored asset is powered off.

Solution

Make sure the monitored asset is on. Enable the connector used to receive data from the monitored asset. Import or create presets that contain tags. To display data on the graph, in the **History** section, select a date, a time interval, and a preset containing tags. To display data in the **Monitoring** section, select a time interval and a preset containing tags.

Events are not transmitted between Kaspersky MLAD and external systems

Problem

Events are not received by Kaspersky MLAD and/or alerts about the monitor activation are not sent to external systems.

Solution

To restore the exchange of events with external systems:

1. Start the Event Processor service and the CEF Connector.
2. When configuring the Event Processor service, do the following:
   a. In the **Event processor configuration file** field, upload the configuration file describing the event parameters.
   b. In the **Interval for receiving batch events (sec.)** field, specify the time interval in seconds required to generate an episode, taking into account the speed of receiving events from the monitored asset.
3. To receive events in the .env file, specify the port number used to connect to the external event source.
4. To send events, when configuring the CEF Connector, specify the IP address and the port number for connecting to the external system.

Cannot load data to view in the Event Processor section

Problem

After restarting Kaspersky MLAD, it is impossible to upload data for viewing the events history and/or pattern history in the **Event Processor** section (the **Process request** button is not available). This problem may also arise after changing the settings of the Event Processor service.

Solution

*To resume uploading of data for viewing the events history and/or pattern history in the **Event Processor** section:*

It is recommended to wait for several minutes. After Kaspersky MLAD is restarted, the state of the Event Processor service is restored. It may take several minutes to restore the state of the service if there is a significantly large number of processed events or registered patterns. Until the state of the Event Processor service is restored in the **Event Processor** section, requests are not fulfilled, data is not updated, and data received from the CEF Connector is not processed. This data is temporarily stored in the system message queue and is processed after the state of the Event Processor service is restored.

Data is incorrectly processed in the Event Processor section

Problem

A large number of short patterns is being created.

Solution

To reduce the number of short patterns registered:

You must increase the episode length in the Event Processor service settings.

Problem

A large number of monitor activation alerts is being received.

Solution

To reduce the number of monitor activation alerts:

Check the previously created monitors and delete the ones that are no longer needed. It is also recommended to update the following monitor activation parameters: **Sliding window** and **Threshold**.

Events are not displayed in the Event Processor section

Problem

When you make a request to view the event history, the **Event Processor**→ **Event history** section does not display the events that were displayed before.

Solution

Make sure that Kaspersky MLAD saves the state of the Event Processor service to the database table.

If the state of the Event Processor service is saved to a file in bit format, Kaspersky MLAD saves the state of the service with the frequency specified in the **Component backup frequency** field. When the Event Processor service is restarted, the results of processing of the event stream received by the Event Processor since the last time the service state was saved are lost.

Previously created monitors and the specified attention settings are not displayed in the Event Processor section

Problem

After restarting or modifying the Event Processor service settings, the **Event Processor**→ **Monitoring** section does not display previously created monitors and the specified attention settings.

Solution

The Event Processor saves the created monitors and the specified attention settings after saving the state of the Event Processor service to a database table or a file in bit format. If Kaspersky MLAD saves the state of the service to a database table, it is recommended not to restart the Event Processor service or change its settings until the first episode of events from the monitored asset is processed, in order to save the created monitors and the specified attention settings. If the application saves the state of the Event Processor service to a file in bit format, it is recommended not to restart the Event Processor service or change its settings until the first backup of the service, in order to save the created monitors and the defined attention settings. The frequency of the Event Processor service backups depends on the value of the **Component backup frequency** setting.

To receive events, configure the settings and start the Event Processor service and the CEF Connector. To process the registered incidents as events, configure and start the Anomaly Detector service and the connector required to receive telemetry data from the monitored asset. Go to the **Dashboard** section and make sure that events are received by Kaspersky MLAD in the online mode.

If the malfunction persists, please contact Kaspersky Technical Support.

A markup result is not displayed

Problem

In the **Models** section, when viewing the markup graph, the data intervals to be selected by the markup appear uncolored.

Solution

The selected time interval may be too short and may not contain enough data for the markup to display the data intervals on the graph. In the **Scale** field, specify a longer time interval to display data on the markup graph.

A Trainer service stopped message is displayed

Problem

When you go to the **Training** tab of an ML model element, you see the **Trainer service is stopped** message. The Trainer service was started by a system administrator or a user with the **Manage statuses of application services** permission from the **Working with application services** permission group.

Solution

Wait approximately two seconds. If the Trainer service is running, the message will disappear automatically.

Training of an ML model element completed with an error

Problem

Training of an ML model element completed with an error. A training error may appear both immediately after training start and after several training epochs are completed.

Solution

If the training of an ML model element completed with an error immediately after training start, make sure that there is data available for all ML model tags within the training interval specified in the **Data selection interval** setting, while considering markup (learning indicator ?). To do this, when changing the training settings, click **On graph** and visually check that at least one data interval selected by the markup is displayed within the defined training interval, and that observations for all tags involved in training the ML model element are displayed within these data intervals.

If the training of an ML model element completed with an error after several epochs, this signifies that the data selected for training may not be suitable for this ML model element. In that case, the target quality metrics of the ML model cannot be achieved. View the graphs on the **Training results** tab and select a different interval to train the ML model element.

The localization language for Help needs to be changed before connecting to the application

Problem

The Help localization language must be changed prior to connecting to the Kaspersky MLAD web interface.

Solution

To change the localization language of the application Help Guide without connecting to the application web interface:

1. Open the browser installed on your computer.
2. In the address bar of the browser, enter the web address of Kaspersky MLAD received from a qualified technical specialist of the Customer, a Kaspersky specialist, or a certified integrator.
3. In the upper-right corner of the account credentials entry page that opens, click the **Help** link.

4. Specify the necessary localization language in the web address:

   - ru – if you want to open Help in Russian (for example, https://<Kaspersky MLAD web address>/help/**ru**/171583.htm).

   - en – if you want to open Help in English (for example, https://<Kaspersky MLAD web address>/help/**en**/171583.htm).

After connecting to the application, you can change the language of the interface and Help in the user menu.

Contacting Technical Support

This section describes the ways to receive technical support, and its terms and conditions.

If you cannot find a solution to your problem in the application documentation or in one of the other sources of information about the application, you are advised to contact Technical Support. Technical Support experts will answer your questions about installing and using the application.

> Technical support services are provided if you have an active *Technical Support Agreement*. The scope of provided technical support services is determined by the current *Technical Support Agreement*.

Before contacting Technical Support, please read the technical support rules.

You can contact Technical Support experts by emailing them at mlad-support@kaspersky.com.

Technical Support experts may request that you provide information from the Kaspersky MLAD logging system.

Limitations

Kaspersky MLAD has a number of limitations that are not critical for application operation:

- Alerts about the activation of the Event Processor service monitors are sent to external systems only using the CEF connector. Sending alerts by email is not available.
- Alerts about the activation of the Event Processor service monitors are not saved in the Kaspersky MLAD database.
- It is recommended to save the Event Processor service state to the database table. If the service state is saved to a file in bit format, Kaspersky MLAD saves the state of the Event Processor service according to the specified backup creation frequency for the service. It may take some time to save and restore the state of the Event Processor service (up to several minutes if there is a large volume of processed data). Restarting the service results in the loss of data since the last time it was saved to a file in bit format.
- The Event Processor service processes only categorical data. All event parameter values are set in or converted to the string data type. Although the string values for each event parameter can be extremely diverse (up to tens of thousands of values), they are finite.
- Data processing performance for the current version of the Event Processor is about five thousand events per second and may decrease due to a large number of attention directions.
- As the stream of events approaches maximum capacity (about five thousand events per second) and the diversity of event parameter values increases, the Event Processor service requires substantial computing resources.
- The Event Processor service is sensitive to how its settings are configured. Incorrectly defined event parameters, episode size and creation time, and attention configuration can significantly reduce service efficiency and performance.
- Kaspersky MLAD is designed to work with a tag stream whose rate does not exceed 10000 tags per second (short-term bursts of no more than 20% are permissible). If the tag stream rate exceeds the specified value, there may be delays in tag processing, prediction, and anomaly detection.
- Computers with Kaspersky MLAD and Kaspersky Industrial CyberSecurity for Networks installed must belong to the same network.
- Kaspersky MLAD stores the entire history of received tag values and predicted tag values. Therefore, you must estimate the potential storage volume based on the data update rate (tags per second) and the time interval for storing the telemetry data monitoring history.
- The Trainer service can only train neural network ML models.
- You can save data during an application update only when updating Kaspersky MLAD 4.0.1-001 or later. To migrate from Kaspersky MLAD 3.0.0 to Kaspersky MLAD 4.0.1 or later, you need to perform a new installation of Kaspersky MLAD and manually import data from the previously installed Kaspersky MLAD 3.0.0. For detailed information on migration from Kaspersky MLAD 3.0.0 to Kaspersky MLAD version 4.0.1 or later, you are advised to contact Kaspersky Technical Support.
- Application rollback to the previously installed version is supported only for Kaspersky MLAD 4.0.1-001 or later.
- If you are using an ML model that consists of multiple elements of the same type, anomalies are not grouped by single-type tags that are associated with different elements of the ML model.
- A large number of simultaneously running ML models (more than 80) can result in the number of connections to the database being exhausted. Restart Kaspersky MLAD if this happens.

- There is no capability to use model elements based on the XGBoost detector.
- In the asset tree, the **Assets** section does not display the icon that is selected when you create or edit tags or assets.
- In the **Incidents** section in the period selection window, you can select only those years for which Kaspersky MLAD contains data.
- The **History** and **Monitoring** sections do not correctly display graphs of tags for which display boundaries on Y coordinate were specified when creating or modifying a tag.
- In the **Models** section, you cannot clone an ML model if it contains no elements or if there is at least one untrained neural network element.
- The **Models** section does not always display the results of training a neural network element after it has been successfully trained. You must refresh the page to display the results.
- The value of the **Monitored asset time zone** setting that is defined by the system administrator in the main settings of Kaspersky MLAD is applied only to dates and times when selecting time intervals for markups. This setting does not apply to other sections of the web interface in which the date and time can be selected for displaying data.

Appendix

This section provides information that supplements the main text of the document.

Settings of a .env configuration file

The settings of the configuration file can be changed only by a qualified technical specialist of the Customer, a Kaspersky employee, or a certified integrator.

The .env configuration file is filled in to configure the CEF Connector and has the settings described in the table below.

Settings of a .env configuration file

Setting	Description
CEF_CONNECTOR_INCOMING_IP	IP address used to connect an external event source to the CEF Connector.
CEF_INCOMING_PORT	Port number used to connect an external event source to the CEF Connector.

To apply changes to the configuration file, restart Kaspersky MLAD.

Settings and example of the Excel file containing tag and asset configuration

The configuration file is created by a qualified technical specialist of the Customer, a Kaspersky employee or a certified integrator. The system administrator loads the configuration of assets and tags into a hierarchical structure in the **Assets** section in the administrator menu.

The configuration file contains the following tabs:

- **readme**: A tab containing general information about the configuration file.
- **directory_types**: A tab that describes the hierarchical structure asset types using the following settings:
  - **directory_type_id**: The asset type ID. The ID is assigned automatically when exporting the asset tree.
  - **directory_type**: A unique name for the asset type.
  - **parameter<parameter number>_label**: Names of special parameters, where <parameter number> corresponds to a value in the range from 1 to 5. If an asset of a given type does not have any special parameter, leave the corresponding field in the configuration file blank.
  - **description**: The description of the asset type. This field is optional.
- **directories**: A tab that describes assets of the hierarchical structure using the following settings:
  - **directory_id**: The asset ID. The ID is assigned automatically when exporting the asset tree.

  - **directory_type**: The type of asset. The type is selected from the asset types specified on the **directory_types** tab.
  - **directory_type row**: The number of the row on the **directory_types** tab that describes the selected asset type. The field is filled in automatically.
  - **directory_name**: The unique name of an asset within its parent asset.
  - **directory_info**: The description of the asset. This field is optional.
  - **parent**: The parent asset. If the imported asset is at the top level of the asset hierarchy, leave the **parent** field blank.
  - **parent row**: The number of the row on which the selected parent asset is described. The field is filled in automatically.
  - **parent_id**: The ID of the parent asset. The ID is assigned automatically when exporting the asset tree.
  - **parameter<parameter number>**: Names of special parameters, where <parameter number> corresponds to a value in the range from 1 to 5. Names of special parameters are filled in automatically if special parameters are defined for the selected asset type.
  - **value <parameter number>**: Values of special parameters, where <parameter number> corresponds to a value in the range from 1 to 5. If an asset does not have a special parameter, leave the field for entering the corresponding value blank.
- **tags**: A tab that describes tags of the hierarchical structure using the following parameters:
  - **tag_id** refers to the tag ID. The ID is assigned automatically when exporting primary elements of the hierarchical structure.
  - **tag_name** is the unique name of the tag.
  - **alternate_name**: A unique alternative name for the tag. This field is optional.
  - **tag_description** refers to a description of the tag.
  - **parent**: The parent asset to which the tag belongs. If the head element of the hierarchical structure is the tag imported by the parent element, leave the **parent** field blank.
  - **parent_row**: The number of the row on the **directories** tab that describes the selected parent asset. The field is filled in automatically.
  - **parent_id**: The ID of the parent asset. The ID is assigned automatically when exporting the asset tree.
  - **tag_type**: Type of tag ?. This field is optional.

- **PV**: To designate measurements or observed values of physical parameters.
- **CV**: To designate calculated values of physical parameters.
- **IV**: To designate tags that are independent of other tags.
- **SV**: To designate a setpoint.
- **MV**: To designate the controlled values of physical parameters.
- **B**: To designate tags in bit format.
- **X**: To designate cases that are not tagged.

If you are finding it difficult to determine the tag type, you can use a question mark (?) as the tag type instead.

- **tag_units**: The unit of measure for the tag.
- **red_min**: Lower blocking threshold, upon reaching which it is necessary for the ICS to take emergency response measures. This field is optional.
- **red_max**: Upper blocking threshold, upon reaching which it is necessary for the ICS to take emergency response measures. This field is optional.
- **yellow_min**: Lower signaling threshold, upon reaching which the operator should pay attention to the tag behavior. This field is optional.
- **yellow_max**: Upper signaling threshold, upon reaching which the operator should pay attention to the tag behavior. This field is optional.
- **validity_min**: The lower threshold for physically possible tag values. This field is optional.
- **validity_max**: The upper threshold for physically possible tag values. This field is optional.
- **display_min**: The lower boundary for displaying tag values on graphs. This field is optional.
- **display_max**: The upper boundary for displaying tag values on graphs. This field is optional.
- **scale**: The expression used to calculate the tag value from the value passed to Kaspersky MLAD. Instead of an expression, you can specify a specific number by which the value of the transmitted tag is to be multiplied. If the tag value does not need to be recalculated, leave this field blank.
- **comment**: A comment relating to the tag.
- **X** is the coordinate of the monitored asset's sensor location. This field is optional.
- **Y** is the Y coordinate of the monitored asset's sensor location. This field is optional.
- **Z** is the Z coordinate of the monitored asset's sensor location. This field is optional.

Below is an example of a XLSX file containing descriptions of assets and tags and their configuration.

Directory_types tab

directory_type_id	directory_type	parameter1_label	parameter2_label	parameter3_label	parameter4_
	Factory	Process	Region		
	Unit	Vendor	Model	Year of manufacture	Responsible
	Setpoints				

Directories tab

directory_id	directory_type	directory_type row	directory_name	directory_info	parent	parent row	paren
	Factory	2	Chemical plant	Tennessee Eastman Process			
	Unit	3	Reactor	Chemical reactor	Chemical plant	2	
	Setpoints	4	Setpoints	Reactor setpoints	Chemical plant; Reactor	3	

tags tab

tag_id	tag_name	alternate_tag_name	tag_description	parent	parent_row	pare
	Reactor_pressure_setpoint		Reactor pressure setpoint	Chemical plant; Reactor; Setpoints	4	
	A_feed_stream1		Reagent consumption A	Chemical plant; Reactor	3	
	No reactor temperature response		Rule	Chemical plant	2	

Example JSON file containing a preset configuration

Below is an example of a JSON file containing descriptions of presets.

Only a qualified Kaspersky employee can create a configuration file. Preset configuration is uploaded by the user in the **Presets** section.

```
{
 "presets": [
 {
 "name": "Product",
 "tag_list": [
 51,
 52,
 53,
 49,
 50
 ],
 "evaluations": {
 "axis_x_name": "",
 "evaluations": []
 },
 "css_class": null,
 "icon": "logout-signout"
 },
...
 {
 "name": "Cooler",
 "tag_list": [
 64
 ],
 "evaluations": {
 "axis_x_name": "",
 "evaluations": []
 },
 "css_class": null,
 "icon": "graph"
 }
 ]
}
```

Example JSON file containing a configuration for the Event Processor service

Below is an example of a JSON file containing a configuration for the Event Processor service. The file contains a description of the event parameters for the Event Processor.

> Only a Kaspersky employee can create a configuration file. The system administrator uploads the Event Processor configuration file when configuring the Event Processor service settings.

```
 {
  "timestamp_field": "TimeStamp",
  "timestamp_scale": "ms",
  "fields": [
  "User_Host",
  "User_Name",
  "Destination_Host",
  "Access_Result"
  ],
  "groupBy": [
  "User_Host",
  "User_Name",
  "Destination_Host",
  "Access_Result"
  ],
  "nodes": [
  {
```

```
  "name": "User_Name",
  "depth": 0,
  "tooltip": {
  "templates": [
  "User: {{User_Name}}"
  ]
  }
  },
  {
  "name": "User_Host",
  "depth": 1,
  "tooltip": {
  "templates": [
  "User host: {{User_Host}}"
  ]
  }
  },
  {
  "name": "Destination_Host",
  "depth": 2,
  "tooltip": {
  "templates": [
  "Destination: {{Destination_Host}}"
  ]
  }
  }
  ],
  "links": [
  {
  "source": "User_Name",
  "target": "User_Host",
  "value": "interval_count",
  "tooltip": {
  "templates": [
  "{{User_Name}} » {{User_Host}}",
  "Count: {{interval_count}}"
  ]
  },
  "isGraphGroup": true
  }, {
  "source": "User_Host",
  "target": "Destination_Host",
  "value": "interval_count",
  "tooltip": {
  "templates": [
  "{{User_Host}} » {{Destination_Host}}",
  "DeviceEventClassID: {{Access_Result}}",
  "Count: {{interval_count}}"
  ]
  }
  }
  ]
 }
```

Viewing the Kaspersky MLAD log

Kaspersky MLAD uses the Grafana logging system to monitor the state of application services and to track information security events.

Tracking information security events of Kaspersky MLAD in the logging subsystem

The table below shows the types of information security events that are tracked in Kaspersky MLAD.

Types of information security events

Information security event ID in the logging system	Information security event type
`login`	Connecting and attempting to connect users to Kaspersky MLAD
`access_control`	Verifying user rights when performing actions in the Kaspersky MLAD web interface
`logout`	Terminating a Kaspersky MLAD user connection
`service_control`	Starting, stopping, and restarting Kaspersky MLAD services
`user_control`	Editing user accounts
`system_settings_control`	Changing Kaspersky MLAD settings
`model_control`	Creating, modifying, and deleting models
`tag_control`	Importing, creating, modifying, and deleting tags
`log_control`	Deleting information security event logs from the Kaspersky MLAD database when the log storage volume is exceeded or when their storage term expires

Each entry about an information security event contains the following parameters:

- **event_id** is the ID of the information security event.
- **timestamp** is the date and time of the information security event.
- **event_type** is the ID of the information security event type.
- **sub_type** specifies the type of information security event.
- **severity** is the importance of the information security event. Kaspersky MLAD provides the following severity levels for information security events:
  - **1** (low).

    These information security events include entries involving users being granted access to perform a specific action in the web interface, and regarding the successful completion of any user actions.
  - **5** (medium).

    These information security events include entries involving user actions in the web interface for managing ML models, tags, user accounts and passwords, and entries regarding exceeded thresholds for storage time and volume of information security event logs.
  - **8** (high).

    These information security events include entries involving users entering an incorrect login and/or password when connecting to the web interface of the application, and entries regarding unsuccessful attempts to change a password.

    - **10** (highest).

      These information security events include entries involving attempts to connect to the application web interface using a system account or a blocked account, and entries regarding attempts to perform specific actions in the application without the appropriate access rights.

- **username** is the name of the user whose actions resulted in the information security event entry.

- **ip_address** is the IP address of the computer from which the user performed the action logged into the information security event log.

- **outcome** is the result of an information security event. The OK result corresponds to successful completion of the operation by the user. The FAIL result corresponds to failure of the user to perform the operation.

- **msg** is a brief summary of the information security event.

- **info** is a detailed description of the information security event.

Tracking the state of Kaspersky MLAD services in the logging subsystem

Kaspersky MLAD services whose states are monitored in the logging subsystem are identified based on the names of their corresponding containers or images in Docker. In most cases, the abbreviated name of the service is used as the name of the image. The container name is formed according to the following template:

`<application directory>-<image name>-#`,

where `#` is the number of the Docker container.

By default, Kaspersky MLAD uses the `mlad-release-4.0.2-<installation build number>` directory.

> The Kaspersky MLAD log stores entries about the state of application services only for the last 48 hours.

The table below presents the correspondence between Kaspersky MLAD services and the names of Docker containers and images.

Correspondence between Kaspersky MLAD services and the names of Docker containers and images

Kaspersky MLAD service	Image name	Container name
Anomaly Detector	anomaly_detector	mlad-release-4.0.2-<installation build number>-anomaly_detector-1
Time Series Database	influxdb	mlad-release-4.0.2-<installation build number>-influxdb-1
Message Broker	kafka	mlad-release-4.0.2-<installation build number>-kafka-1
Keeper	keeper	mlad-release-4.0.2-<installation build number>-keeper-1
Logger	logger	mlad-release-4.0.2-<installation build number>-logger-1
Database	postgres	mlad-release-4.0.2-<installation build number>-postgres-1
Similar Anomaly	similar_anomaly	mlad-release-4.0.2-<installation build number>-similar_anomaly-1
Event Processor	event-processor	mlad-release-4.0.2-<installation build number>-event-processor-1

Stream Processor	stream-processor	mlad-release-4.0.2-<installation build number>-stream-processor-1
Trainer	trainer	mlad-release-4.0.2-<installation build number>-trainer-1
Web Server	nginx-ui	mlad-release-4.0.2-<installation build number>-nginx-ui-1
API Server	web-server	mlad-release-4.0.2-<installation build number>-web-server-1
Mail Notifier	postman	mlad-release-4.0.2-<installation build number>-postman-1
OPC UA Connector	opcua-connector	mlad-release-4.0.2-<installation build number>-opcua-connector-1
MQTT Connector	mqtt-connector	mlad-release-4.0.2-<installation build number>-mqtt-connector-1
AMQP Connector	amqp-connector	mlad-release-4.0.2-<installation build number>-amqp-connector-1
HTTP Connector	gate	mlad-release-4.0.2-<installation build number>-gate-1
KICS Connector	kics3-connector	mlad-release-4.0.2-<installation build number>-kics3-connector-1
CEF Connector	cef-connector	mlad-release-4.0.2-<installation build number>-cef-connector-1
WebSocket Connector	ws-connector	mlad-release-4.0.2-<installation build number>-ws-connector-1
	webstatic	mlad-release-4.0.2-<installation build number>-webstatic-1
	migrations	mlad-release-4.0.2-<installation build number>-migrations-1

The `Info` logging level is used for the Time Series Database, Message Broker, Logger, Database and Web Server services, and for webstatic and migrations images. The logging levels for all other Kaspersky MLAD services are defined by the system administrator when configuring the application settings.

Scenario: viewing information security event logs

Before starting to work with the logging subsystem, it is recommended to read the Grafana User Guide.

The maximum volume and storage time for information security event entries are defined when configuring the security settings.

Information security event logs are written to the Kaspersky MLAD database automatically. If necessary, the system administrator can specify the settings of an external system to which the information security event logs should be sent.

The scenario for viewing information security event logs consists of the following steps:

1. **Navigating to the logging subsystem**

   Navigate to the logging system by clicking the button ▤

   Available only to the system administrators and users with the **Working with application logs** permission.

2. **Navigating to the section containing information security event logs**

   Go to the **Security audit** section.

3. **Analyzing information security event logs**

   Analyze the information security event log entries for the selected period. You can filter them based on parameters of the information security event logs. To do so, click the filtering icon (▼) in the column containing the relevant log parameter, select the check boxes next to the necessary filtering criteria, and click **OK**. To reset the filtering criteria, clear the relevant check boxes and click **OK**.

4. **Exporting information security event logs**

   To export the information security event logs for the selected period to a text file, in the **Security audit** section, use the **Security audit** drop-down list above the information security event log table to select **Inspect** → **Data**, and click the **Download CSV** button in the opened pane.

Scenario: assessing the main metrics of Kaspersky MLAD

Before starting to work with the logging subsystem, it is recommended to read the Grafana User Guide .

When connecting to the logging subsystem for the first time, you must change the default password.

This subsection provides a sequence of actions that must be performed to assess the health and general state of Kaspersky MLAD.

The scenario for assessing the health and general state of Kaspersky MLAD consists of the following steps:

1. **Navigating to the logging subsystem**

   Navigate to the logging system by clicking the button

   Available only to the system administrators and users with the **Working with application logs** permission.

2. **Analyzing the main metrics of Kaspersky MLAD**

   In the **Summary docker metrics** section, analyze the graphs of the main Kaspersky MLAD metrics for the selected period.

   The following metrics are displayed for each container of Kaspersky MLAD services:

   - *CPU usage* – history of central processor workload caused by the container. This is measured as a percentage.
   - *RAM usage* – history of the container's RAM usage. This is measured in bytes.
   - *Disk usage* – history of the container's load on the disk subsystem (read/write operations). This is measured in bytes.
   - *Network usage* – history of the container's use of network resources. This is measured in bytes per second.

Scenario: viewing container logs and metrics

Before starting to work with the logging subsystem, it is recommended to read the Grafana User Guide.

The Kaspersky MLAD log stores entries only for the last 48 hours.

This subsection provides steps for assessing the performance and viewing the logs of a specific container from the Kaspersky MLAD distribution kit.

The scenario for assessing the performance and viewing the logs of a specific container consists of the following steps:

1. **Navigating to the logging subsystem**

   Navigate to the logging system by clicking the button

   Available only to the system administrators and users with the **Working with application logs** permission.

2. **Navigating to the section with container logs and metrics**

   Go to the **Service detailed monitoring** section and select the relevant container from the **Container** drop-down list.

3. **Analyzing container metrics**

   In the **Service detailed monitoring** section, analyze the graphs of Kaspersky MLAD metrics for the selected container during the relevant period.

   The **Service detailed monitoring** section provides the following metrics:

   - *Memory* – history of the container's RAM usage. This is measured in bytes.
   - *CPU* – history of central processor workload caused by the container. This is measured as a percentage.
   - *File system* – history of the container's load on the disk subsystem (read/write operations). This is measured in bytes.
   - *Network* – history of the container's use of network resources. This is measured in bytes per second.

4. **Analyzing container logs**

   Analyze the container log records for the selected period, which are displayed under the metrics dashboard. You can search the container log records. To do so, enter a search query in the **Log search** field and press the **ENTER** key. To reset the search results, clear the **Log search** field and press the **ENTER** key.

5. **Exporting container logs**

   To export container logs for the selected period to a text file, in the **Service detailed monitoring** section, select **Inspect** → **Data** from the **Service log** drop-down list and click **Download CSV** in the opened pane.

Special characters of regular expressions

You can use regular expressions to search for events, patterns and values of event parameters in the **Event Processor** section. Kaspersky MLAD supports use of the following special characters in regular expressions:

- `^` – Corresponds to the start of the parameter value. For example, `^A` means that the event parameter search will look for values beginning with the letter A.
- `$` – Corresponds to the end of the parameter value. For example, `A$` means that the event parameter search will look for values ending with the letter A.
- `.` – Corresponds to any single character.
- `|` – Splits permissible options for characters or a set of characters in a parameter value. For example, `c(o|a)t` matches both the `cot` and `cat` values.
- `\` – Indicates that the next character is an ordinary character (not a special character) in the parameter value. You can use the `\` character to search for special characters in a parameter value. For example, `\.` describes a dot in the parameter value, while `\\` describes a backslash.
- `[]` – Corresponds to any character from the set of permissible characters. For example, `[ abc ]` matches the occurrence of any one of the three specified characters.

  To search for a range of values, you can use the `-` character. To find the characters that are not within the specified range, you can use the `^` character in the square brackets. For example, `[^0-9]` means any character except numerals can be present.

You can use the following special characters to indicate the necessary number of repetitions of an expression in the values of event parameters:

- `?` – Character indicating that the preceding expression may occur zero or one time in a parameter value.
- `*` – Character indicating that the preceding expression may occur zero or more times in a parameter value.
- `+` – Character indicating that the preceding expression may occur one or more times in a parameter value.
- `{}` – Character class that lets you indicate the necessary number of repetitions of the preceding expression. You can specify the repetition count in one of the following ways:
  - `{n}` – The expression preceding the curly brackets occurs in the parameter value exactly `n` times.
  - `{m,n}` – The expression preceding the curly brackets occurs in the parameter value from `m` to `n` times inclusive.
  - `{m,}` – The expression preceding the curly brackets occurs in the parameter value at least `m` times.
  - `{,n}` – The expression preceding the curly brackets occurs in the parameter value no more than `n` times.

You can also use parentheses `()` to group elements of an expression. For example, `( c[oa]t ){2}` matches `cotcot`, `catcat`, `cotcat`, and `catcot`.

Cipher suites for secure TLS connection

It is recommended to use the following cipher suite for a secure TLS connection via the TLS-1.2 protocol:

- 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_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256;
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.

It is recommended to use the following cipher suite for a secure TLS connection via the TLS-1.3 protocol:

- TLS_AES_128_GCM_SHA256;
- TLS_AES_256_GCM_SHA384;
- TLS_CHACHA20_POLY1305_SHA256;
- TLS_AES_128_CCM_SHA256.

Glossary

Account role

Set of access rights that determine the actions available to a user when connected to the application web interface. Kaspersky MLAD includes a system administrator role and user roles.

AMQP topic

A hierarchical path to the data source used for sending messages via the AMQP protocol.

Anomaly

Any deviation in the behavior of a monitored asset that is abnormal, unexpected, and not prescribed by the industrial process.

Asset

A section of a hierarchical structure representing, for example, a plant, a shop, or a separate unit of a monitored asset.

Attention

A special configuration of the Event Processor intended to track events and patterns for specific subsets of event history (attention directions). An attention direction is defined by the event parameter value that is common for all events of this direction. The Event Processor detects events and patterns only for the attention directions defined in the attention settings.

Connector

Service that facilitates the exchange of data with external systems.

Data sampling

A method for adjusting the training set with reference to the time scale steps in the original dataset.

Detector

Component in the ML model that identifies anomalies and registers incidents.

Event

Set of values describing a change in the state of a monitored asset based on a predefined list of parameters, with the timestamp of the change.

Gradient boosting

Machine learning technique for classification and regression problems that builds a prediction model in the form of an ensemble of prediction models, which are typically decision trees (XGBoost).

ICS

Abbreviation for Industrial Control System. A package of hardware and software designed to automate control of process equipment at industrial enterprises.

Incident

A deviation from the expected (normal) behavior of a monitored asset identified by the anomaly detector.

Inference

The ML model works with telemetry data to detect anomalous behavior.

Inference indicator

A set of criteria used to determine the data time intervals on which the ML model performs the inference.

Learning indicator

A set of criteria used to determine the data time intervals on which the ML model performs the training.

Markup

A set of time intervals specified for tags that allows you to generate learning indicators and inference for the ML model.

ML model

Algorithm based on machine learning methods tasked with analyzing the telemetry of the monitored asset and detecting anomalies.

ML model branch

Determines how the predicted tag value, personal tag error and MSE are calculated. For a complex model, the calculation may involve multiple ML model elements that have a different composition of tags and error calculation parameters.

Monitor

Source of notifications about patterns, events, or values of event parameters detected by the Event Processor according to the defined monitoring criteria. The monitoring criteria define a sliding time interval, the number of sequential detections, filters for event parameter values, and the condition for detecting new events, patterns, or event parameter values.

Monitored asset hierarchical structure

A method of organizing monitored asset data in the form of a tree, whose leaf nodes correspond to source tags and/or tags processed by the Stream Processor service.

MQTT topic

A hierarchical path to the data source used for sending messages via the MQTT protocol.

Notification

A message containing information about an incident (or incidents) that is sent by the application via notification delivery systems (for example, by email) to the specified addresses.

Pattern

Sequence of events or other patterns identified within the stream of events from the monitored asset.

Preset

Set of tags generated by a user in arbitrary order or created automatically when an incident is registered. A set of tags in a custom preset can correspond to a certain aspect of the technological process or a section of the monitored asset.

Tag

Variable that contains the value of a specific process parameter such as temperature.

Top tag

Process parameter for which the largest deviation from the prediction was recorded at the time of incident registration.

Uniform temporal grid (UTG)

An infinite sequence of points in time separated by equal intervals, to which the stream of incoming telemetry data is converted.

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt located in the application installation directory (in the 'legal' subdirectory).

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Ubuntu and LTS are registered trademarks of Canonical Ltd.

The Grafana Word Mark and 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 the permission of Coding Instinct. We are not affiliated with, endorsed or sponsored by Coding Instinct, or the Grafana community.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights described in other terms used in this document.

Google Chrome is a trademark of Google LLC.

TensorFlow and any related marks are trademarks of Google LLC.

Intel, Core, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft and Excel are trademarks of Microsoft Corporation.

Python is a trademark or registered trademark of Python Software Foundation.

PGP is a trademark or registered trademark of Symantec Corporation or its affiliates in the United States and elsewhere.