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 3.0.0 (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 cyber-physical 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 the users about the detected incidents using the web interface, by email, by sending messages in 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 to create templates based on the added ML models and add ML models to Kaspersky MLAD based on the created templates.
- 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 mlad-3.0.0-<build number>.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" folder 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.

To ensure proper operation of Kaspersky MLAD, your computer must meet the following minimum requirements.

Requirements for Kaspersky MLAD server

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
- 1 TB of free space on the hard drive (SSD recommended)

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™ 2.8.3 library:

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

Supported operating system:

- Ubuntu® 22.04 LTS and 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.

Operator computer requirements

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

- Intel Core™ i5 CPU;
- 8 GB of RAM;
- 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

Important! ML model parameters directly impact the detection of anomalies, therefore they can only be changed by Kaspersky MLAD 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 also 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 your administrator.
- Ensure protection of traffic within the intranet system.
- Ensure protection of connections to external networks.
- For connections through the web interface, use passwords that contain at least 8 characters, including letters and numerals. Ensure that passwords are confidential and unique. If a password has been potentially compromised, change the password (in the current version of the application, only an administrator can change a password).
- Set a time limit for a user web session.
- After you are finished working in the browser, manually terminate the application connection session 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 also take the following measures to ensure data security:

- 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 the activation code and sensitive data in a secure storage location.

Managing access to application functions

This section describes user access restrictions for application functions.

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.

Available functions of the application depending on the user role

Application function	Administrator	Operator
Managing user accounts	✓	
Assigning roles to users	✓	
Viewing the roles and rights of users	✓	
Managing incident notifications	✓	
Receiving and processing incident notifications	✓	✓
Configuring Kaspersky MLAD	✓	
Importing and exporting tag configurations	✓	
Managing tags	✓	
Monitoring of process parameters in real time	✓	✓
Viewing historical data (including the capability to select the date and scale).	✓	✓
Viewing registered incidents and incident groups	✓	✓
Importing (presets sections only) and exporting presets	✓	✓
Managing presets	✓	✓
Managing ML models and ML model templates	✓	
Viewing ML model details	✓	✓
Configuring attention settings and display of event parameters	✓	

Viewing the events history	✓	✓
Viewing the pattern history	✓	✓
Managing monitors	✓	✓
Viewing Kaspersky MLAD services	✓	✓
Managing Kaspersky MLAD services	✓	
View Kaspersky MLAD logs.	✓	

You can view the available user roles under **Settings** → **Roles**. The **Roles** section contains a table that provides **information about each role**.

- **ID** is the digital ID of the user role.
- **Role** is the name of the user role (Administrator or Operator).
- **Activity** indicates whether this role is in use.
- **Description** refers to a description of the user role.
- **Created at** refers to the date and time when the user role was created.
- **Updated at** refers to the date and time when the user role was updated.

You can view application functionality access rights under **Settings** → **Permissions**. The **Permissions** section contains a table that provides **information about users' permissions to access application functions**.

- **ID** is the digital identifier of the right to access application functions.
- **Code** is the internal code of the right to access application functions.
- **Description** refers to a description of the right to access application functions.

User roles and access rights can be viewed only by users that have administrator privileges.

What's new

Kaspersky Machine Learning for Anomaly Detection 3.0.0 introduces the following features and improvements:

- **Models** section of the web interface – the functionality for creating templates based on ML models and adding ML models based on the created templates is implemented. ML model templates preserve the algorithm structure, set of elements, and the training state of the ML model used to create the template.

- Stream Processor service – a new component is added for converting telemetry data received from the monitored asset at arbitrary real-time moments to a uniform temporal grid (UTG). The Stream Processor component considers possible data losses and processes observations received by Kaspersky MLAD too early or too late. In such cases, Stream Processor registers incidents.

- Event Processor service – the functionality that switches the Event Processor to the sleep mode according to a specified schedule is implemented. In the sleep mode, the Event Processor analyses sequences of events processed in the online mode once again to improve the quality of previously detected patterns and their structure. A mechanism for saving the Event Processor service state in the database after processing each episode of events is implemented. This mechanism ensures that the data is saved up to the last processed episode and reduces the need for computational resources required to save the full state of the Event Processor service. The functionality is added that allows you to view the structure of patterns as a layered hierarchy of nested elements, including the time intervals between the elements within the pattern.

- WebSocket Connector – a new connector is added that allows you to receive telemetry data from ICS systems and send messages about incident registration via the WebSocket protocol.

- **System parameters** section of the web interface – the functionality for managing logging levels of Kaspersky MLAD services, statuses and causes of incidents, and time intervals for displaying data on graphs in the **Monitoring**, **History**, and **Time slice** sections is implemented. The functionality for managing the user account blocking settings is added.

- **Tags** section of the web interface – the function is implemented to automatically add unknown tags received from external assets via the KICS Connector in accordance with the names of tags and assets in Kaspersky Industrial CyberSecurity for Networks 3.0 and later.

Basic concepts of Kaspersky MLAD

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

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.

- **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.

- **Virtual tags**

  The values of these tags are calculated based on the values of the source tags or tags received by the Stream Processor service, according to the formula specified when the virtual tag was created. Virtual tags can be created to visualize data on graphs. These tags are not saved in the database.

  Virtual tags can be a useful tool for detecting anomalies and for analyzing telemetry data, including for analyzing the state and quality of industrial processes. For example, you can predict the value of the "product quality" virtual tag based on the actual values of the source tags.

- **Indicator tags**

  The values of these tags are generated by the Rule Detector, which operates based on diagnostic rules. They reflect the state of fulfillment (triggering) of one or more diagnostic rules.

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 by Kaspersky experts or a certified integrator 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 loaded into Kaspersky MLAD to work with a monitored asset 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. Normally, the more complex the industrial processes of the monitored asset are, the more elements the ML model will contain.

A Kaspersky MLAD ML model can be built using one or more detectors running in parallel:

- **Forecaster** ?.

  > 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. 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.

- **Rule Detector** ?.

This detector uses diagnostic rules to detect anomalies. 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 formulated by subject-area experts and are implemented by Kaspersky experts or a certified integrator in the form of software modules written in Python. 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.

- **Limit Detector**.

  Limit Detector is a special type of ML model element, which registers incidents whenever a tag value falls below the minimum value or exceeds the maximum value. The Limit Detector uses the minimum and maximum permissible values specified in the tag description for the monitored asset. In this case, machine learning is not applied.

- **XGBoost**.

  If an expert markup of anomalous time intervals and types of anomalies in historical data is available, a widely used machine learning method known as "supervised learning" can be used to train an ML model. XGBoost performs gradient boosting over decision trees. Training this type of ML model results in an XGBoost classifier that determines the probability of detecting anomalies in the data of a monitored asset.

  In monitoring mode, an ML model that is based on the XGBoost detector displays a graph of the adjusted probability of anomaly detection. The XGBoost detector registers an incident and identifies the type of incident if the probability exceeds the defined threshold.

  > An ML model based on the XGBoost detector is provided by Kaspersky experts when specially requested.

In Kaspersky MLAD, an ML model can be imported or created based on a template. In turn, ML model templates are created based on previously added ML models. ML model templates preserve the algorithm structure, set of elements, and the state of the ML model used to create the template. The 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.

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. 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 components of Kaspersky MLAD.

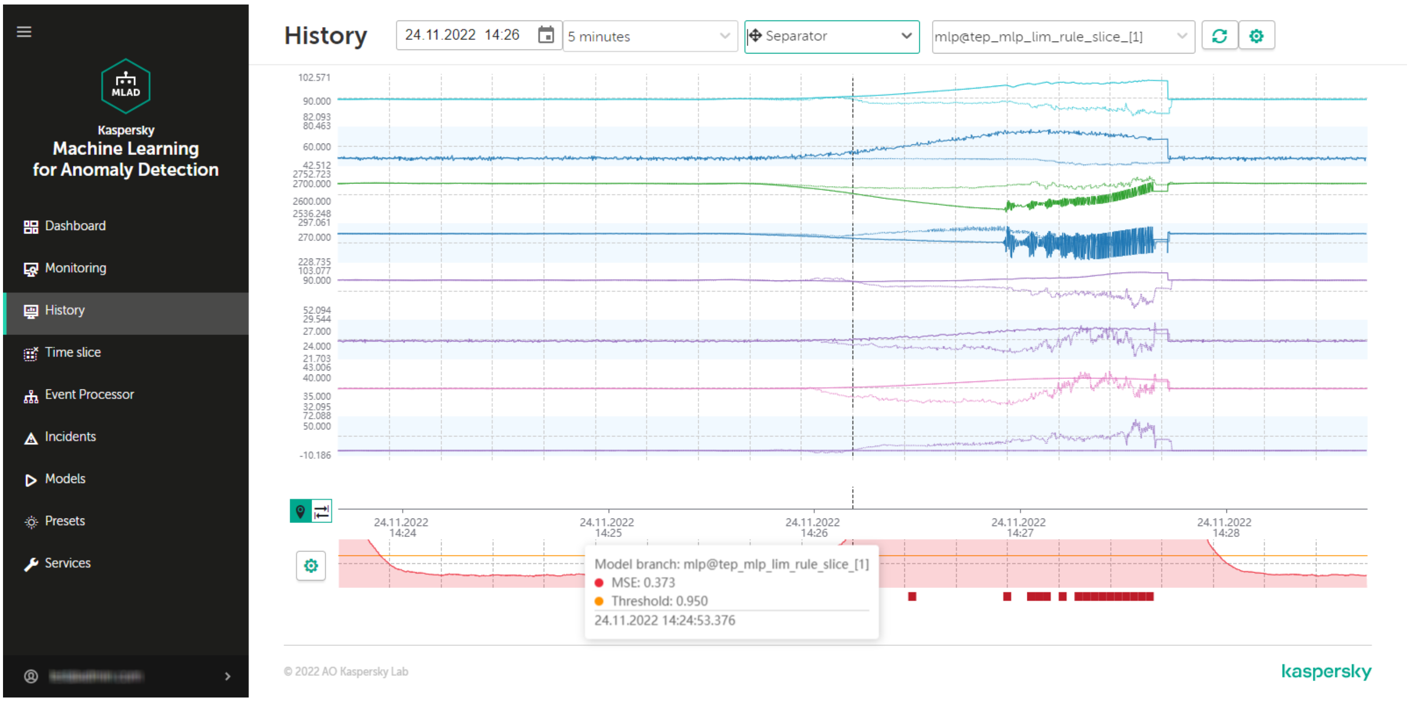
Incidents detected by the Forecaster detector

An ML model created 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 (in_tags parameter) and which tags' behavior is predicted (out_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).



Model branch: mlp@tep_mlp_lim_rule_slice_[1]
● MSE: 0.373
● Threshold: 0.950
24.11.2022 14:24:53.376

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 the Rule Detector

An ML model element based on the *Rule Detector* consists of one or several diagnostic rules. Each diagnostic rule results in a value of an indicator tag that is calculated at each point in time. The name and description of the indicator tag represent the purpose of the diagnostic rule, for example, *Sensor X failure*, *Dirty turbine blades*, and *Rotor speed drop*. You can interpret the values of an indicator tag as follows:

- The value `0` was received. The diagnostic rule was not triggered or applied at this moment.
- The value `1` was received. 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 value of an indicator tag reaches the threshold defined for a diagnostic rule (normally equal to 1), the Rule Detector registers an incident. The indicator tag is displayed in the incidents table in the **Incidents** section. 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 includes the indicator tag that invoked the incident, and the tags that are included in the corresponding diagnostic rule.

To display the graphs of indicator tags, you can enable display of predicted tag values in the **History** section.

Incidents detected by the Limit Detector

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

To visually control the position of a tag graph relative to its technical limits, enable the **Always show technical limits** option. If this option is disabled, the upper or lower limit line is displayed only if the tag values reached the corresponding limit during the time interval displayed on the screen. The Limit Detector identifies and registers events regardless of whether or not the **Always show technical limits** 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 technical limits of tag values 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. When gathering 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:

- **Monitored asset time failure** – 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.

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 by the administrator 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 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 components

Kaspersky MLAD includes the following components:

ML model

An *ML model* is a model created by Kaspersky experts or by a certified integrator 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 is not included in the application distribution kit but is provided as part of the *Kaspersky MLAD Model-building and Deployment Service*.

Kaspersky MLAD services

Kaspersky MLAD services comprise the set of main application components 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.
- *Model 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*. Performs data exchange between Kaspersky MLAD components.
- *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 3.0 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 the components of Kaspersky MLAD.

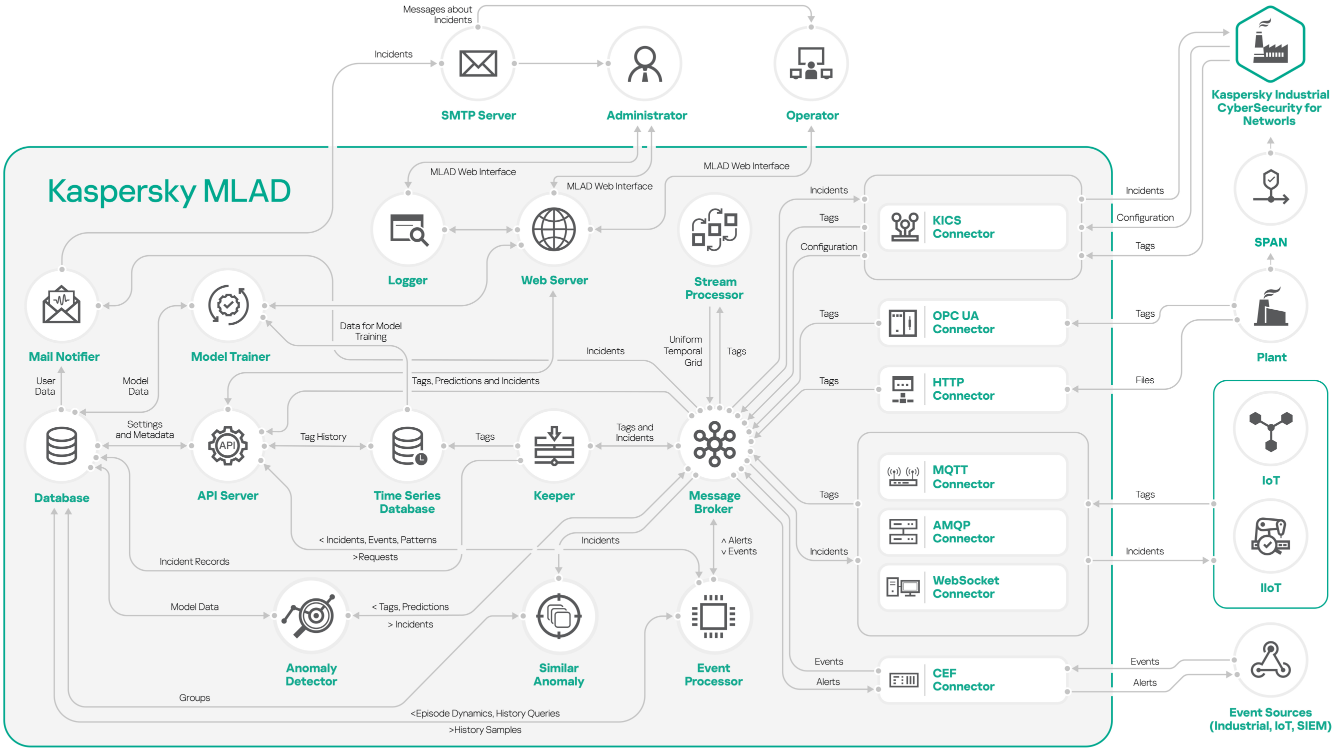


Diagram of interaction of Kaspersky MLAD components

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:

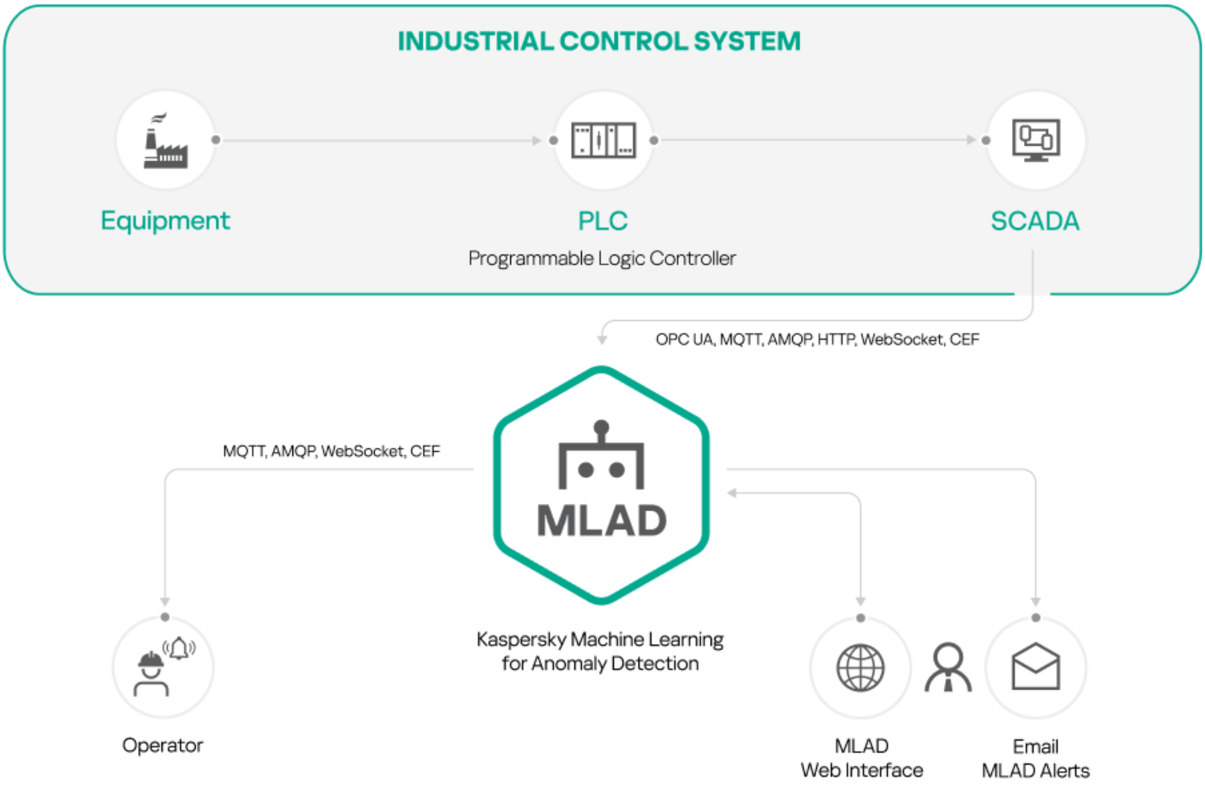
- Standalone installation.
- Installation with Kaspersky Industrial CyberSecurity for Networks version 3.0 and later.

Standalone installation of Kaspersky MLAD

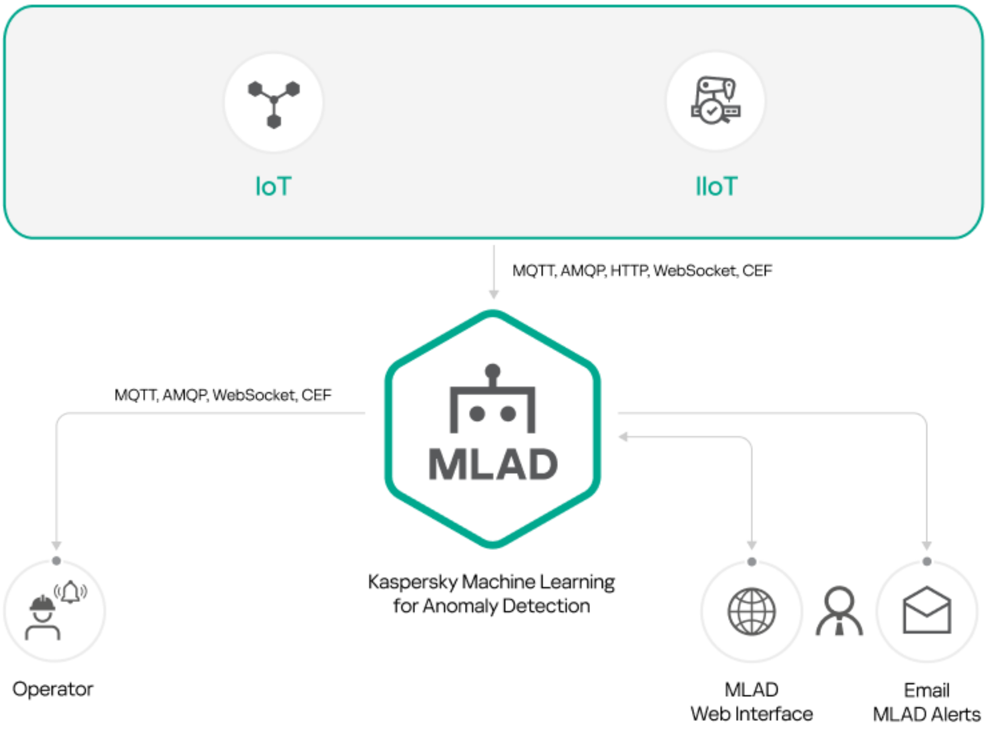
You can install only Kaspersky MLAD if you plan to use the following connectors as a data provider:

- 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

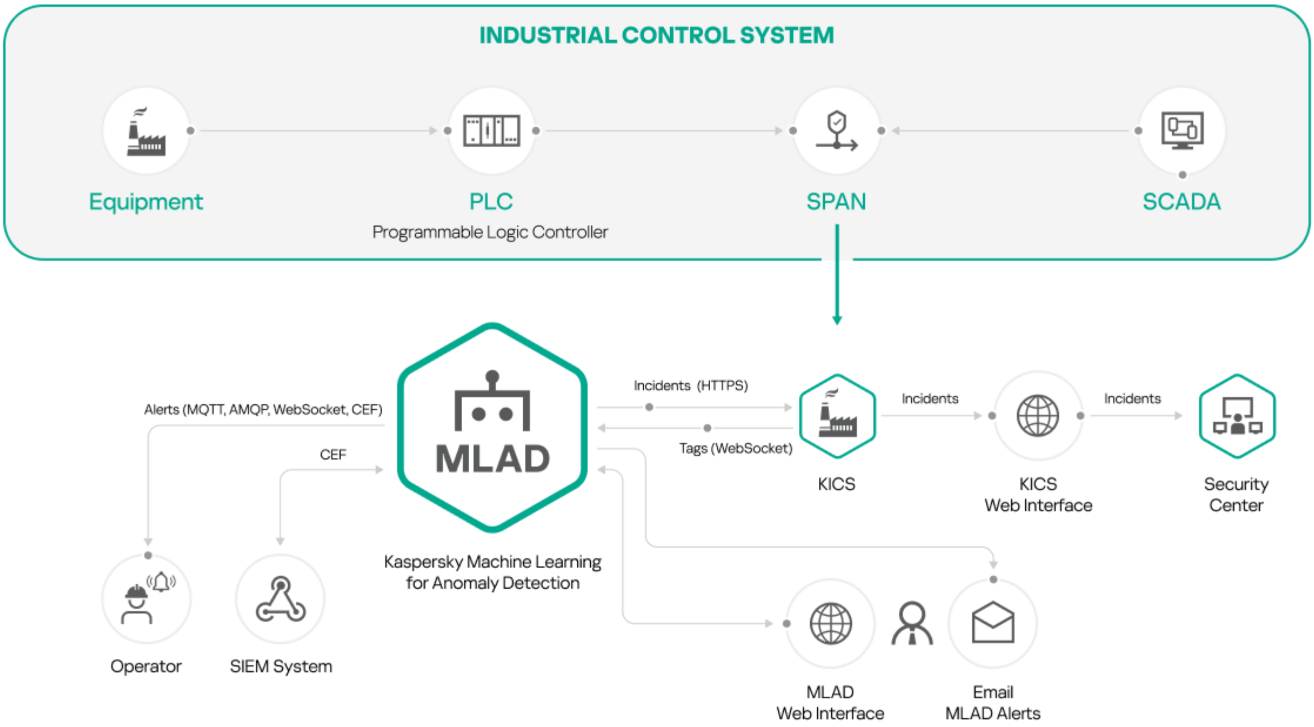
Standalone installation of Kaspersky MLAD using connectors: OPC UA Connector, MQTT Connector, AMQP Connector, HTTP Connector, WebSocket Connector


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 3.0 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 can configure the HTTP Connector, MQTT Connector, AMQP Connector, OPC UA Connector, KICS Connector, CEF Connector, and WebSocket Connector.

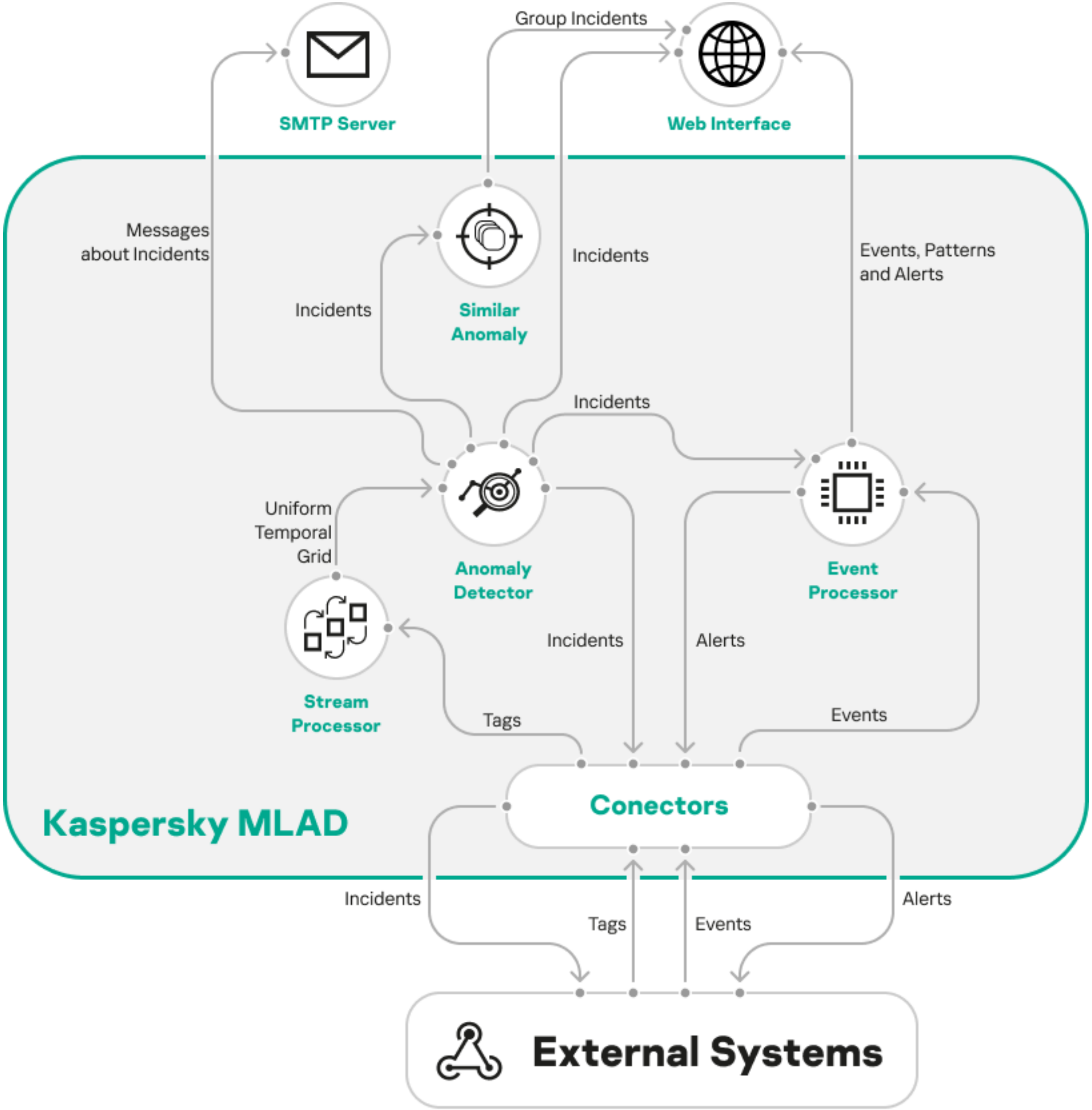
The Stream Processor service performs the initial processing of the telemetry data of the monitored asset, converting the received tags to a uniform temporal grid (UTG). When Stream Processor service detects loss of telemetry data and observations received by Kaspersky MLAD too early or too late, it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

Administering Kaspersky MLAD

This section provides information on installing, updating, configuring, and removing the application. This section also provides instructions on managing user accounts and incident notifications.

Installing the application

This section contains options for installing the application (normal mode and silent mode), and a step-by-step description of Kaspersky MLAD installation for each of the options.

> Installation of Kaspersky MLAD is performed by a qualified administrator that is employed by the Customer and authorized to accept the End User License Agreement for the application.

To install Kaspersky MLAD from the command line:

1. Unpack the archive named mlad-3.0.0-<build number>.tar.xz that is included in the distribution kit:

   ```
   tar xf mlad-3.0.0-<build number>.tar.xz
   ```

2. Navigate to the directory named mlad-release-3.0.0-<build number>:

   ```
   cd mlad-release-3.0.0-<build number>
   ```

3. Run the setup.sh installation script:

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

4. Follow the instructions of the Application Setup Wizard.

To install Kaspersky MLAD in non-interactive mode:

1. Unpack the archive named mlad-3.0.0-<build number>.tar.xz that is included in the distribution kit:

   ```
   tar xf mlad-3.0.0-<build number>.tar.xz
   ```

2. Navigate to the directory named mlad-release-3.0.0-<build number>:

   ```
   cd mlad-release-3.0.0-<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.

   `-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' folder.

As a result, the application is installed on the computer.

Updating the application and rolling back to the previous installed version

This section contains a step-by-step description of how to update Kaspersky MLAD, and a description of how to roll back the application to the previous installed version.

Update and rollback of Kaspersky MLAD are possible only for application versions 3.0.0-001 or later. 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.

Kaspersky MLAD must be updated by a qualified administrator who is employed by the Customer and authorized to accept the End User License Agreement for Kaspersky MLAD.

To update Kaspersky MLAD from the command line:

1. Unpack the archive named mlad-3.0.0-<new build number>.tar.xz that is included in the distribution kit:

   ```
   tar xf mlad-3.0.0-<new build number>.tar.xz
   ```

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

   ```
   cd mlad-3.0.0-<new build number>
   ```

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

   ```
   sudo ./upgrade.sh
   ```

   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.

As a result, Kaspersky MLAD will be updated to the version specified in the build number. All application files are located in the folder where Kaspersky MLAD is installed (mlad-release-3.0.0-<installation build number> by default). A directory named upgrade_backup-3.0.0-<previous build number> will also be created there and will contain a backup copy of the previous version of Kaspersky MLAD. It is not recommended to move the upgrade_backup-3.0.0-<previous build number> directory to a different directory.

To roll back Kaspersky MLAD to the previous installed version:

1. Go to the directory that contains the backup copy of Kaspersky MLAD:

   ```
   cd upgrade_backup-3.0.0-<previous build number>
   ```

2. Run the application update script named upgrade.sh with the `-r` switch:

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

3. Follow the instructions of the Application Upgrade Wizard.

> 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.

As a result, Kaspersky MLAD will be rolled back to the previous installed version.

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 (optional) their presets are prepared as a JSON file to be imported into Kaspersky MLAD. This file is created by Kaspersky experts or a certified integrator.
5. An ML model or multiple ML models are created, trained on historical telemetry data, and prepared to be imported into Kaspersky MLAD as TAR files. These files are created by Kaspersky experts or a certified integrator.
6. The Kaspersky MLAD 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

> Kaspersky MLAD starts automatically immediately after installation.

To start the application after it has been stopped:

1. Go to the folder where Kaspersky MLAD is installed (mlad-release-3.0.0-<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 folder where Kaspersky MLAD is installed (mlad-release-3.0.0-<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-3.0.0-<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 administrator – a Customer employee authorized to accept the End User License Agreement for the application.

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-3.0.0-<installation build
number>/ssl/nginx/mlad_nginx.crt
sudo cp <new certificate key.key> mlad-3.0.0-<installation build
number>/ssl/nginx/mlad_nginx.key
```

The new certificate and its key are saved to the mlad-3.0.0-<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-3.0.0-<installation build number>/mlad-stop.sh
mlad-3.0.0-<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.

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 3.0 and later.

First startup of Kaspersky MLAD

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

Kaspersky MLAD starts automatically immediately after installation.

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 login and password that were created by default. 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 **Settings** → **System parameters** section, 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 tag configuration to Kaspersky MLAD and creating presets**

A tag configuration is created by a Kaspersky expert or integrator while deploying the application and building an ML model. A tag configuration is described in a JSON file. An example configuration description is provided in the Appendix.

For subsequent operation, upload a tag configuration to Kaspersky MLAD. If your tag configuration does not contain presets, create new presets from tags.

5 **Uploading and activating an ML model**

> 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*.

Upload and activate the 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.

Completion of these steps should result in the following:

- 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.

Configuring Kaspersky MLAD

This section contains instructions on configuring Kaspersky MLAD settings.

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.

> Configuration of the main parameters of Kaspersky MLAD is performed by an administrator (Kaspersky employee or certified integrator).

To configure the main settings of Kaspersky MLAD:

1. In the administrator menu, select **System parameters** → **Main**.

   A list of options appears on the right.

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

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

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

5. 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.

6. 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.

7. 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.

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

9. 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.

> Configuration of the Anomaly Detector service is performed by an administrator (Kaspersky employee or certified integrator).

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

1. In the administrator menu, select **System parameters** → **Anomaly Detector**.

   A list of options appears on the right.

2. Move the **Use Limit Detector** toggle button to the necessary position to enable or disable use of the Limit Detector.

3. Move the **Use Forecaster detector** toggle button to the necessary position to enable or disable use of the Forecaster detector.

4. Move the **Use XGBoost detector** toggle button to the necessary position to enable or disable use of the XGBoost detector.

5. Move the **Use Rule Detector** toggle button to the necessary position to enable or disable use of the Rule Detector.

6. Move the **Skip gaps in data** toggle button to the necessary position to enable or disable the function for skipping gaps in the incoming data stream.

7. 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.

8. 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.

9. 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.

10. 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.

> Configuration of the Kaspersky MLAD data routing settings is performed by an administrator (Kaspersky employee or certified integrator).

To configure the Kaspersky MLAD data routing settings:

1. In the administrator menu, select **System parameters** → **Keeper**.

   A list of options appears on the right.

2. 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.

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

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

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

6. 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.

> Configuration of the Mail Notifier service is performed by an administrator (Kaspersky employee or certified integrator).

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 administrator menu, select **System parameters** → **Mail Notifier**.

   A list of options appears on the right.

2. If necessary, move the **Use SSL connection** toggle button to enable the use of a secure SSL connection.

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

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

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

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

6. If you are using a secure SSL connection:

   - In the **SMTP server certificate** field, upload the Certification Authority certificate.

   - In the **Key to SMTP server certificate** field, upload the key to the Certification Authority certificate.

   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.

7. 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.

Configuration of the Similar Anomaly service is performed by an administrator (Kaspersky employee or certified integrator).

To configure the Similar Anomaly service:

1. In the administrator menu, select **System parameters** → **Similar Anomaly**.

   A list of service settings appears on the right.

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

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

   If you want all incidents to be put into one group, leave this field empty.

4. 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`.

5. 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).

Configuration of the Stream Processor service is performed by an administrator (Kaspersky expert or certified integrator).

To configure the Stream Processor service:

1. In the administrator menu, select **System parameters** → **Stream Processor**.

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

3. In the **Configuration file** field, add the file containing the 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 (⤓).

4. 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.

Configuration of the HTTP Connector is performed by a Kaspersky employee or certified integrator.

To configure the HTTP Connector:

1. In the administrator menu, select **System parameters** → **HTTP Connector**.

A list of options appears on the right.

2. Use the **Write data to the Message Broker service** toggle button to enable writing data to the Message Broker service.

3. If necessary, move the **Save received file** toggle button to enable the function for saving received CSV files.

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

5. 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.

   If `0` is defined, the maximum file size is unlimited.

6. Click the **Save** button.

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

An example of sending a CSV file to the HTTP Connector via cURL 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.

Configuration of the MQTT Connector is performed by a Kaspersky employee or certified integrator.

To configure the MQTT Connector:

1. In the administrator menu, select **System parameters** → **MQTT Connector**.

   A list of options appears on the right.

2. If necessary, move the **Use SSL connection** toggle button to enable the use of a secure SSL connection.

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

3. 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`.

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

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

6. If you enabled the use of a secure SSL connection, add the root certificate for the MQTT broker in the **CA certificate** field.

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

7. If you need to use client certificates for a secure SSL connection, perform the following actions:

   - In the **Client certificate** field, add the MQTT client application certificate.

   - In the **Key to client certificate** field, add the key for the MQTT client application certificate.

   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.

8. 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`.

9. 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.

10. 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.

11. If you selected `Topic` data type, in the **Connector configuration file** field, add a configuration file containing the connector settings for this data format.

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

12. 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 button.

    By default, scaling of the received data is disabled.

13. 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).

> Configuration of the AMQP Connector is performed by a Kaspersky employee or certified integrator.

To configure the AMQP Connector:

1. In the administrator menu, select **System parameters** → **AMQP Connector**.

   A list of options appears on the right.

2. If necessary, move the **Use SSL connection** toggle button to enable the use of a secure SSL connection.

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

3. 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`.

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

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

6. If you enabled the use of a secure SSL connection, add the root certificate for the AMQP broker in the **CA certificate** field.

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

7. If you need to use client certificates for a secure SSL connection, perform the following actions:

   - In the **Client certificate** field, add the AMQP client application certificate.

   - In the **Key to client certificate** field, add the key for the AMQP client application certificate.

   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.

8. 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 `/`.

9. 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.

10. 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 `#`.

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

12. 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 8 of these instructions.

    This setting has no value by default.

13. 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`.

14. 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.

15. If you selected `Topic` data type, in the **Connector configuration file** field, add a configuration file containing the connector settings for this data format.

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

16. 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 button.

    By default, scaling of the received data is disabled.

17. 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.

> Configuration of the OPC UA Connector is performed by a Kaspersky employee or certified integrator.

To configure the OPC UA Connector:

1. In the administrator menu, select **System parameters** → **OPC UA Connector**.

   A list of options appears on the right.

2. In the **Connection point** field, specify the connection address. For example, `opc.tcp://10.65.48.40:8001/freeopcua/server/`.

3. In the **Configuration file** field, add the file containing the OPC UA Connector configuration settings.

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

4. Click the **Save** button.

Kaspersky MLAD will receive data using a protocol described by the OPC Unified Architecture specification.

Configuring the KICS Connector

Kaspersky MLAD uses the KICS Connector to receive data from Kaspersky Industrial CyberSecurity for Networks 3.0 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*.

Integration with Kaspersky Industrial CyberSecurity for Networks 3.0 and later is performed by a Kaspersky employee or certified integrator.

To configure the KICS Connector:

1. In the administrator menu, select **System parameters** → **KICS Connector**.

   A list of options appears on the right.

2. In the **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 (⬇).

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

4. 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 button.

5. 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.

6. 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 button.

   By default, scaling of the received data is disabled.

7. 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 (Industrial Internet of Things, network devices and applications) and to return messages regarding incident registration.

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 to the external event source for receiving events must be specified in the .env file.

Configuration of the CEF Connector is performed by a Kaspersky employee or certified integrator.

To configure the CEF Connector:

1. In the administrator menu, select **System parameters** → **CEF Connector**.

   A list of options appears on the right.

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

3. To send messages about the incidents registered by the Anomaly Detector service to an external system, enable the **Send registered incidents to SIEM system** option.

4. 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.

5. In the **IP address for sending events and incidents to SIEM system** field, specify the IP address for connecting to the external system and forwarding events processed by the Event Processor service and incidents registered by the Anomaly Detector service.

6. In the **Port for sending events and incidents to SIEM system** field, specify the port number for connecting to the external system and forwarding events processed by the Event Processor service and incidents registered by the Anomaly Detector service.

7. Click the **Save** button.

Kaspersky MLAD receives data from external sources of events (Industrial Internet of Things, network devices, and applications) and returns messages about the registration of events and incidents.

Configuring the WebSocket Connector

Kaspersky MLAD uses the WebSocket Connector to receive data and send messages about incident registration via the WebSocket protocol.

Configuration of the WebSocket Connector is performed by a Kaspersky employee or certified integrator. The instructions in this section are provided for information purposes.

To configure the WebSocket Connector:

1. In the administrator menu, select **System parameters** → **WebSocket Connector**.

   A list of options appears on the right.

2. In the **WebSocket server web address** field, specify the web address of the WebSocket server that the WebSocket Connector will interact with.

   Indicate the web address in the format `WebSocket protocol://address:port/`.

3. To use a secure connection to connect to the WebSocket server, add the root certificate for the WebSocket server in the **CA certificate** field.

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

4. To use client certificates for a secure connection to the WebSocket server, do the following:

   - In the **Client certificate** field, add the certificate of the WebSocket client application.

   - In the **Key to client certificate** field, add the key for the WebSocket client application certificate.

   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.

5. 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.

6. If you selected `Topic` data type, in the **Connector configuration file** field, add a configuration file containing the connector settings for this data format.

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

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 button.

   By default, scaling of the received data is disabled.

8. To send alerts about the incidents registered in Kaspersky MLAD to a WebSocket server, enable the **Submit incidents** option.

9. 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.

> Configuration of the Event Processor service is performed by an administrator (Kaspersky expert or certified integrator).

To configure the Event Processor service:

1. In the administrator menu, select **System parameters** → **Event Processor**.

   A list of service settings appears on the right.

2. In the **Online mode** section, do the following:

   a. In the **Event processor configuration file** field, add the file containing the configuration settings for the Event Processor service.

   This configuration file is created by a Kaspersky expert or 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 button.

   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 select to store the Event Processor service state in a file in bit format, in the **File containing a backup copy of the component state** field, add the file containing a backup copy of the Event Processor service.

   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.

3. 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.

- **Sends 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.

4. 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.

> Configuration of the causes and statuses of incidents is performed by an administrator (Kaspersky employee or certified integrator).

To add statuses of incidents:

1. In the administrator menu, select **System parameters** → **Incidents**.
2. In the **Statuses of incidents** section, click the **Create** button.

   The **Create element** pane will appear on the right.

3. In the **Value, in Russian** field, specify the name of the incident status in Russian.

4. In the **Value, in English** field, specify the name of the incident status in English.

5. 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.

6. 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.

7. 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.

> Configuration of Kaspersky MLAD service logging is performed by an administrator (Kaspersky employee or certified integrator).

To configure the log levels of Kaspersky MLAD services:

1. In the administrator menu, select **System parameters** → **Logging**.

   The list of Kaspersky MLAD services will be displayed on the right.

2. 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.

3. 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.

> Configuration of time intervals for displaying data on graphs is performed by an administrator (Kaspersky employee or certified integrator).

To add time intervals for displaying data:

1. In the administrator menu, select **System parameters** → **Graphs**.
2. In the **Time intervals** settings group, click the **Create** button.

   The **Create element** pane will appear on the right.
3. 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.
4. If necessary, change the Russian name of the time interval in the **Value, in Russian** field.
5. If necessary, change the English name of the time interval in the **Value, in English** field.
6. 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.
7. 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

Configuration of the display settings for the main menu of Kaspersky MLAD is performed by an administrator (Kaspersky employee or certified integrator).

To configure how the main menu and the administrator menu of Kaspersky MLAD are displayed:

1. In the user menu, select the **Settings** section.

   You will switch to administrator mode.

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 button to enable or disable the display of a specific section in the main menu.

4. In the **Availability of menu items in administrator mode** settings group, use the toggle button to enable or disable the display of a specific section in the administrator menu.

5. Click the **Save** button.

Exporting and importing a configuration file for Kaspersky MLAD components

Kaspersky MLAD lets you export and import a configuration file containing the settings for application components that 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.

To export a components configuration file from Kaspersky MLAD:

1. In the administrator menu, select **System parameters**.

2. Click the **Export** button in the upper part of the opened page.

The Kaspersky MLAD components configuration file will be saved as an archive named mlad-settings.tar.gz on the local computer.

To upload a components configuration file 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 components.

The Kaspersky MLAD components configuration file will be uploaded to the application.

Starting, stopping, and restarting services

Kaspersky MLAD lets you start, stop and restart services.

Kaspersky MLAD services can be managed only by users with administrator privileges.

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.

Managing tags

Tags management is available only for users with administrator privileges.

In the **Settings** → **Tags** section, you can view tags and tag groups that were created in or uploaded to Kaspersky MLAD. The structure of tags and tag groups is displayed as a tag tree. For each tag, the tree shows the ID, name, and description. You can create tags and tag groups, and edit tag parameters, such as permissible technical limits of tag values 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. When saving of all tags is enabled, the Time Series Database also saves IDs and values of unknown tags (not listed in the tag tree). You can compare the current tag structure to the tag structure in the Time Series Database and add missing tags to the current structure, if necessary.

If Kaspersky MLAD detects unknown tags received from external assets via the KICS Connector, these tags are automatically created in the **Settings** → **Tags** section in accordance with the names of tags and assets in Kaspersky Industrial CyberSecurity for Networks.

Kaspersky MLAD is compatible with Kaspersky Industrial CyberSecurity for Networks version 3.0 and later.

You can also delete existing tags, import tags from a JSON file, or export them to a JSON file.

Create tag

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 administrator menu, select **Tags**.
2. In the upper part of the page, click the **Create** button.

   The **Create tag** pane opens on the right.
3. In the **Tag type** drop-down list, select **Tag**.
4. If necessary, click the **Choose an 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. In the **Group** drop-down list, select the desired tag group to which you want to assign the created tag.

   Tag groups must be previously loaded or created manually.
6. Specify the 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.

   If the use of the KICS connector is enabled, Kaspersky MLAD automatically fills in the tag name based on the tag name received from Kaspersky Industrial CyberSecurity for Networks.
7. Enter a description for the tag in the **Description** field.
8. Enter the tag ID in the **ID** field.
9. In the **Dimension** field, specify the measurement units for the tag.
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 **Class to display** field, specify the class for displaying the tag.
12. In the **Technical limits** section, in the **Lower** and **Upper** fields, specify the lower and upper limits for the tag values.

    These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower technical limit, the Limit Detector registers an incident.

    If the **Always show technical limits** option is enabled, the vertical scale of the graph will be defined by limit 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 limits, the vertical scale will be automatically changed to display the tag values exceeding the limits.

13. 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 technical limits, even if the **Always show technical limits** function is enabled.

14. In the **Asset** field, specify the name of the asset created in the external system, for which you need to receive tags.

    If the use of the KICS connector is enabled, Kaspersky MLAD automatically fills in the asset name based on the asset name for which the tag is received from Kaspersky Industrial CyberSecurity for Networks.

15. If you need to add additional horizontal threshold lines for this tag on graphs in the **Monitoring** and **History** sections, click the **Add line** button and use the **Threshold value** field to enter the value that should be displayed on the graph.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

16. Click the **Create** button.

The new tag will appear under **Tags** in the tag tree on the left. If necessary, you can change the position of tags in the tag tree. To do this, drag the required tag up or down in the tag tree by the three horizontal lines (≡) to the left of its ID.

Creating a virtual tag

You can create virtual tags in Kaspersky MLAD.

To calculate the real and predicted values of a virtual tag, and the virtual tag error, you can define expressions with simple arithmetic operations (such as addition, subtraction, multiplication, and division), calculation of the square root (the sqrt function) and exponentiation (using the ^ character). You can use the following variables in your expressions:

- *$tag* is the value of the tag based on which the value of the virtual tag is calculated.
- *$tagX* is the X coordinate of the monitored asset's sensor location.
- *$tagY* is the Y coordinate of the monitored asset's sensor location.
- *$tagZ* is the Z coordinate of the monitored asset's sensor location.

For example, you can specify an expression to calculate the Celsius temperature based on the tag that receives the Fahrenheit temperature:

```
5/9 * ($tag - 32)
```

The values of the virtual tag will be displayed on the graphs in the **Monitoring** and **History** sections in accordance with the specified expression.

To create a new tag:

1. In the administrator menu, select **Tags**.

2. In the upper part of the page, click the **Create** button.

   The **Create tag** pane opens on the right.

3. In the **Tag type** drop-down list, select **Virtual tag**.

4. If necessary, click the **Choose an icon** button and select an icon for the virtual 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. In the **Group** drop-down list, select the tag group to which you want to assign the created virtual tag.

   Tag groups must be previously loaded or created manually.

6. in the **Name** field, specify the virtual tag name.

7. In the **Description** field, specify the virtual tag description.

8. In the **ID** field, specify the virtual tag ID.

9. In the **Dimension** field, specify the measurement units for the virtual tag.

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 coordinate values to calculate virtual tag values and display them on graphs in the **Monitoring** and **History** sections.

11. In the **Class to display** field, specify the class for displaying the virtual tag.

12. In the **Technical limits** section, in the **Lower** and **Upper** fields, specify the lower and upper limits for the virtual tag values.

    These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower technical limit, the Limit Detector registers an incident.

    If the **Always show technical limits** option is enabled, the vertical scale of the graph will be defined by limit 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 limits, the vertical scale will be automatically changed to display the tag values exceeding the limits.

13. In the **Display boundaries** section, in the **Lower** and **Upper** fields, specify the lower and upper limits for displaying the virtual tag values on the 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 technical limits, even if the **Always show technical limits** function is enabled.

14. In the **Asset** field, specify the name of the asset created in the external system, for which you need to calculate the virtual tag values.

15. If you need to add additional horizontal threshold lines for this tag on graphs in the **Monitoring** and **History** sections, click the **Add line** button and use the **Threshold value** field to enter the value that should be displayed on the graph.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

16. To display the values of a virtual tag on the graphs in the **Monitoring** and **History** sections, perform the following actions in the **Tag calculation expression** group of settings:

   a. In the **Calculation tag ID** drop-down list, select the ID of the tag based on which you want to calculate the value of the virtual tag.

   b. In the **Expressions for calculating actual and predicted tag values** drop-down list, select one of the following values:

      - If you want to use the same expressions to calculate the actual and predicted tag values, select **Identical expressions**.

      - If you want to use different expressions to calculate the actual and predicted tag values, select **Different expressions**.

   c. In the **Expression for calculating tag values** field, specify an expression for calculating tag values.

      This field is displayed if you chose to calculate actual and predicted tag values using the same expressions.

   d. In the **Expression for calculating actual tag values** field, specify an expression for calculating actual tag values.

      This field is displayed if you chose to calculate actual and predicted tag values using different expressions.

   e. If necessary, enter a tag value calculation expression for predicted values in the **Expression for calculating predicted tag values** field.

      This field is displayed if you chose to calculate actual and predicted tag values using different expressions.

   f. If necessary, enter an expression for error calculation in the **Error calculation expression** field.

17. Click the **Create** button.

   The new tag will appear under **Tags** in the tag tree on the left. If necessary, you can change the position of tags in the tag tree. To do this, drag the required tag up or down in the tag tree by the three horizontal lines (≡) to the left of its ID.

Creating a group of tags

In Kaspersky MLAD, you can create tag groups and categorize tags as you see fit. For example, you can create tag groups for the assets of the monitored asset from which telemetry data is received.

Tag groups are used to represent the tag structure as a tag tree.

To create a new tag group:

1. In the administrator menu, select **Tags**.

2. In the upper part of the page, click the **Create** button.

   The **Create tag** pane opens on the right.

3. In the **Tag type** drop-down list, select the **Group** value.

4. If necessary, click the **Choose an icon** button and select an icon for the tag in the opened window.

   You can upload the tag group 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 group icon, click the icon and then click **Delete** in the opened window.

5. In the drop-down list, select the tag group that will be used as the basis for creating a new tag group.

6. In the **Name** field, enter a name for the tag group.

7. In the **Description** field, provide a description for the tag group.

8. Click the **Create** button.

   The new tag group will appear under **Tags** in the tag tree on the left. If necessary, you can change the position of the tag group in the tag tree. To do this, drag the required group of tags up or down in the tag tree holding by the three horizontal lines (☰) to the left of the tag group name.

Editing a tag

You can edit previously created tags.

To edit a tag:

1. In the administrator menu, select **Tags**.

2. In the tag tree on the left, select the tag you want to edit and click **Edit**.

   You can also switch to the tag edit mode by double-clicking the tag.

   The **Edit tag** pane opens on the right.

3. If you need to change the icon of the tag, click the **Choose an 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. If necessary, enter a new name for 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.

   If the use of the KICS connector is enabled, Kaspersky MLAD automatically fills in the tag name based on the tag name received from Kaspersky Industrial CyberSecurity for Networks.

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

6. If necessary, enter new measurement units for the tag in the **Dimension** field.

7. 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 coordinate values to calculate virtual tag values and display them on graphs in the **Monitoring** and **History** sections. You can also use sensor coordinates to calculate tag values when creating a preset and displaying them on the graph in the **Time slice** section.

8. In the **Class to display** field, specify the class for displaying the tag.

9. In the **Technical limits** section, in the **Lower** and **Upper** fields, specify the lower and upper limit boundaries for tag values.

   These settings are required for correct operation of the Limit Detector. Whenever the tag value reaches its upper or lower technical limit, the Limit Detector registers an incident.

If the Always show technical limits option is enabled, the vertical scale of the graph will be defined by limit 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 limits, the vertical scale will be automatically changed to display the tag values exceeding the limits.

10. 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 technical limits, even if the Always show technical limits function is enabled.

11. In the **Asset** field, specify the name of the asset created in the external system, for which you need to receive tags.

    If the use of the KICS connector is enabled, Kaspersky MLAD automatically fills in the asset name based on the asset name for which the tag is received from Kaspersky Industrial CyberSecurity for Networks.

12. If you need to add additional horizontal threshold lines for this tag on graphs in the **Monitoring** and **History** sections, click the **Add line** button and use the **Threshold value** field to enter the value that should be displayed on the graph.

    Additional horizontal threshold lines help visually evaluate the fluctuations of tag values within certain limits. You can add multiple additional horizontal threshold lines.

13. If you want to modify the expression used to calculate virtual tag values, do the following in the **Tag calculation expression** group of settings:

    a. In the **Expressions for calculating actual and predicted tag values** drop-down list, select one of the following values:

       - If you want to use the same expressions to calculate the actual and predicted tag values, select **Identical expressions**.

       - If you want to use different expressions to calculate the actual and predicted tag values, select **Different expressions**.

    b. In the **Expression for calculating tag values** field, specify an expression for calculating tag values.

       This field is displayed if you chose to calculate actual and predicted tag values using the same expressions.

    c. In the **Expression for calculating actual tag values** field, specify an expression for calculating actual tag values.

       This field is displayed if you chose to calculate actual and predicted tag values using different expressions.

    d. In the **Expression for calculating predicted tag values** field, specify an expression for calculating predicted tag values.

       This field is displayed if you chose to calculate actual and predicted tag values using different expressions.

    e. In the **Error calculation expression** field, specify an expression for error calculation.

14. Click the **Save** button.

The modified tag will appear under **Tags** in the tag tree on the left. If necessary, you can change the position of tags in the tag tree. To do this, drag the required tag up or down in the tag tree by the three horizontal lines (≡) to the left of its ID.

Editing a group of tags

You can edit previously created tag groups.

To edit a tag group:

1. In the administrator menu, select **Tags**.
2. In the tag tree on the left, select the tag group you want to edit and click **Edit**.

   You can also switch to the edit tag group mode by double-clicking the tag group.

   The **Edit tag group** pane opens on the right.
3. If you need to change the icon of the group, click the **Choose an icon** button and select an icon for the tag group in the opened window.

   You can upload the tag group 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 group icon, click the icon and then click **Delete** in the opened window.
4. If necessary, enter a new name for the tag group in the **Name** field.
5. If necessary, provide a new description for the tag group in the **Description** field.
6. Click the **Save** button.

The modified tag group will appear under **Tags** in the tag tree on the left. If necessary, you can change the position of the tag group in the tag tree. To do this, drag the required group of tags up or down in the tag tree by the three horizontal lines (≡) to the left of the tag group name.

Removing a tag or group of tags

You can move previously created tags and tag groups from the tag tree to the tag trash bin and permanently delete them from the trash bin. To remove a tag or tag group:

1. In the administrator menu, select **Tags**.
2. In the tag tree or in the trash bin, select the check boxes next to the name of the tag or tag group.

   To remove one or several tags from a group, expand the tag group by clicking the right arrow (›) and select the required tags. You can also select all tags and groups at the same time by selecting the check box in the table header.
3. Click the **Delete** button in the upper part of the page.
4. In the opened **Confirm deletion** window, click **Yes** to confirm deletion.

If the selected tags and tag groups were in the tag tree during deletion, these tags will be moved to the trash bin. To restore tags, select tags and tag groups in the trash bin and drag these tags and groups from the trash bin to the desired location in the tag tree by the three horizontal lines (≡) to the left of one of the selected items.

If the selected tags and tag groups were in the trash bin during deletion, they will be permanently deleted from Kaspersky MLAD.

Checking the current structure of tags

Kaspersky MLAD saves the tags received from external assets in the Time Series Database. When unknown tags are received via the KICS Connector, the application also automatically creates these tags in the **Settings** → **Tags** section.

Kaspersky MLAD allows you to compare the current tag structure displayed in the **Settings** → **Tags** section and used for a monitored asset to the one saved for this monitored asset in the Time Series Database. 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:

1. In the administrator menu, select **Tags**.

2. In the upper part of the page, click the **Compare tags** button.

   The current tag structure used for the monitored asset is compared with the tag structure stored in the Time Series Database. 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.

3. To add missing tags, do the following:

   a. For each detected tag, in the **Group** field select the group to which you want to assign the tag.

   b. Click **Yes**.

Kaspersky MLAD adds the tags to the current tag structure. Only the IDs, names in the **Tag <tag ID>** format, and the groups to which the tags are assigned are specified for these tags. If necessary, you can change the added tags.

Uploading a tag configuration to the system

> A tag configuration is created while deploying Kaspersky MLAD and building an ML model. A tag configuration is supplied in a JSON file.

To upload a tag configuration to Kaspersky MLAD:

1. In the administrator menu, select **Tags**.

2. Click the **Import** button.

3. In the opened window, select the JSON file containing the necessary tag configuration.

A tag configuration can be uploaded to Kaspersky MLAD. Tags grouped by industrial units are displayed as a tree in the left part of the **Tags** section.

Saving a tag configuration to a file

You can save the structure of tags and presets to a JSON file for subsequent use.

To save a tag configuration to a JSON file:

1. In the administrator menu, select **Tags**.
2. Click the **Export** button.

   The tag configuration will be saved to a file named mlad.json (see the example in the Appendix).

Managing ML models and templates

The **Models** section provides data on ML models and on the templates created based on the ML models added to Kaspersky MLAD.

ML models and templates can be managed only by the users with administrator privileges.

Models tab

The **Models** tab shows a table of ML models. You can upload ML models to Kaspersky MLAD or add ML models based on ML model templates.

The following information is displayed for each ML model:

- **ID** – digital identifier of the ML model.
- **Model name** – name of the added ML model.
- **Creation method** – indicator of whether the ML model was imported, created from a template, or created as a result of training on a previously added ML model. If the template used to create the ML model is deleted, the **Creation method** column shows the **Template deleted** value. If the ML model used to train the current ML model is deleted, the **Creation method** column shows the **Cloned and trained; original model deleted** value.
- **State** – toggle button allowing you to enable or disable the use of the ML model for the monitored asset. If an ML model is not activated, the **State** column shows an inactive **Unavailable** toggle button.
- **Action** – button for activating the ML model or starting the ML model training process after activation.

Next to each model, there is a vertical menu ⋮, allowing you to create a template based on the existing ML model, view detailed information about the model, or delete the ML model.

Templates tab

The **Templates** tab provides a table of templates that were created based on ML models added to Kaspersky MLAD. The following information is available for each template:

- **ID** – digital identifier of the ML model template.
- **Template name** – name of the ML model template.
- **Creation method** – name of the ML model used to create the template. If the ML model used to create the template is deleted, the **Creation method** column shows the **Original model was deleted** value.
- **Action** – button for creating an ML model based on a template.

You can use created templates to add new ML models to Kaspersky MLAD. After adding an ML model, you can enable its use for the monitored asset. You can also delete ML model templates.

Editing the parameters of an ML model and its elements

You can edit certain parameters of an ML model and its elements.

> The parameters of an ML model and ML model element can be changed only by a Kaspersky employee or certified integrator. It is not recommended to change these parameters on your own.

To change the parameters of an ML model:

1. In the main menu, select the **Models** section.
2. Click the vertical menu ⋮ next to the ML model whose parameters you want to change, and select **Model details**.

   The **<ML model name>** pane opens on the right showing the **Model parameters** tab.
3. Click the **Edit** button.
4. On the **Model parameters** tab, edit the relevant parameters of the ML model.
5. On the **Model elements** tab, edit the parameters of the relevant ML model element. If you need to change the relative weights for output tags of an ML model element, do the following:

   a. In the list of parameters of the ML model element, click the **out_tags and mse_weights** parameter value.

      The **Output tags and their relative weights** pane is displayed on the right.

   b. Click the **Edit** button.

   c. Change the values of relative weights in the **Weight value** column for the relevant output tags of the ML model element and click **Save**.

   d. Click the **Close** button.
6. Click the **Save** button.

Uploading an ML model

Kaspersky MLAD lets you upload new ML models. ML model files for uploading are provided by Kaspersky experts or a certified integrator.

Kaspersky MLAD may slow down its operation when uploading an ML model whose size exceeds 1 GB.

To upload an ML model:

1. In the main menu, select the **Models** section.
2. Click the **Import** button.
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 name and state of the ML model are displayed in the table. Activate the ML model after uploading. If you upload an ML model that was previously activated and then deleted, you do not need to reactivate the ML model.

Activating an ML model

After adding a new ML model to Kaspersky MLAD, you have to activate the model before you can use it.

If the ML model activation code is lost, send a request to Kaspersky to receive a new code.

To activate an ML model:

1. In the main menu, select the **Models** section.
2. In the **Action** column, click **Activate**.

   The **Model activation** pane 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 lower part of the window.

ML model is activated. You need to enable an ML model to start the analysis of telemetry data received from the monitored asset.

Changing the status of an ML model

You can enable or disable the use of an ML model for analyzing telemetry data from the monitored asset. After activation, an ML model is disabled by default.

By default, Kaspersky MLAD supports the parallel operation of five ML models. If required, a user with administrator privileges can change the maximum number of simultaneously running models when configuring the Anomaly Detector service.

To change the status of an ML model:

1. In the main menu, select the **Models** section.

2. Use the toggle button in the **State** column to enable or disable the use of the relevant ML model.

   You can enable or disable the use of an ML model that was previously activated. If an ML model is not activated, the **State** column shows an inactive **Unavailable** toggle button.

Training an ML model

Kaspersky MLAD lets you clone an existing ML model built with a Forecaster detector in order to retrain it or perform additional training based on new telemetry data obtained by Kaspersky MLAD for a specific monitored asset.

> Training an ML model is a resource-consuming process. Depending on the model complexity and the amount of data, the main Kaspersky MLAD services (data reception, anomaly detection, web interface operation) may slow down. To clarify the rules for training the ML model, it is recommended to consult with Kaspersky experts or a certified integrator.

To train an ML model:

1. In the main menu, select the **Models** section.

2. In the **Action** column, click the **Train** button located next to the ML model that you want to use as the base for training the new ML model.

   The **Model cloning and training** pane opens on the right.

3. If necessary, enter a name for the new ML model in the **New model name** field.

   By default, a new ML model is assigned a name in the following format: <original model name>_Cloned&Retrained_<date and time>.

4. In the **Start of the data export period** field, click the **Calendar** icon (📅) and select the start date and time of the data export period for training the model.

5. In the **End of the data export period** field, click the **Calendar** icon (📅) and select the end date and time of the data export period for training the model.

6. Expand the **Additional settings** list by clicking the right arrow (›), and, if necessary, specify values for the following settings:

   - In the **Number of training epochs** field, specify the number of training epochs.

     Kaspersky MLAD can finish training the ML model before the specified number of epochs is reached, if it considers that the ML model is trained. The default number is 10000 training epochs.

   - To limit the time for training the model, enable the **Limit the model training time** option and fill in the following fields:

     - In the **Days** field, specify the number of days to train the ML model.

     - In the **Hours** field, specify the number of hours to train the ML model.

   - Perform one of the following actions:

     - If you want to load the relative weights of the output tags of a previously trained ML model, enable the **Load the pre-training state of the original model** option.

  - If you want to retrain the ML model, disable the **Load the pre-training state of the original model** option.

  This option is disabled by default.

- In the **Error resolution window** field, specify an MSE smoothing interval (alpha parameter).

  By default, this interval is equal to the forecast window size **forecast_window_size**. If MSE smoothing is not required, enter 0 in the **Error resolution window** field.

  > Only Kaspersky experts or a certified integrator can change the error smoothing interval.

7. Click the **Clone and train** button.

After training, the new ML model will appear in the models table.

Removing an ML model

You can remove one or more ML models from Kaspersky MLAD.

> After an ML model is removed, the results of the tag values predicted using this model and the calculated MSE are unavailable.

To remove an ML model:

1. In the main menu, select the **Models** section.
2. In the model table, select one or more ML models and click **Delete**.

   You can also remove a specific ML model by selecting **Delete** in the vertical menu ⋮ for the relevant model.
3. Confirm deletion of the ML model.

The selected ML model will be removed from Kaspersky MLAD.

Creating a template based on an ML model

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.

To create a template based on an ML model:

1. In the main menu, select the **Models** section.
2. Click the vertical menu ⋮ next to the ML model that you want to use as the basis for creating the template.
3. Select **Create template**.

   The **Creating a template** pane opens on the right.

4. Enter the template name in the **Template name** field.

   You can enter up to 100 characters.

5. 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 under **Settings** → **Tags**, 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 **Test <Model tag ID>**.

   You can specify a template tag name different from the tag names in the **Settings** → **Tags** section. Template tags and tags in the **Settings** → **Tags** 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 **Create** button.

The created ML model template is displayed on the **Templates** tab.

Creating an ML model based on a template

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 and click **Templates**.

2. In the **Action** column, click the **Create model** button in the row of the template you want to use as the basis for creating the ML 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 ID** column, select the tag IDs for each tag of the created ML model.

   Template tags and tags in the **Settings** → **Tags** section are mapped based on the IDs of the ML model tags.

5. Click the **Create** button.

The newly created ML model is displayed on the **Models** tab. 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

You can remove an ML model template from Kaspersky MLAD.

To remove an ML model template:

1. In the main menu, select the **Models** section and click **Templates**.

2. In the templates table, select one or more ML model templates and click the **Delete** button.

   You can also remove a specific ML model template by selecting **Delete** from the vertical menu ⋮ in the row of the relevant template.

3. Confirm deletion of the ML model template.

   The selected ML model template will be removed from Kaspersky MLAD. Deleting a template does not remove ML models based on this template.

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.

Only the users with administrator privileges can manage 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** 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 button 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.

Managing user accounts

This section contains information about managing Kaspersky MLAD user accounts.

Kaspersky MLAD user accounts can be managed only by users that have administrator privileges.

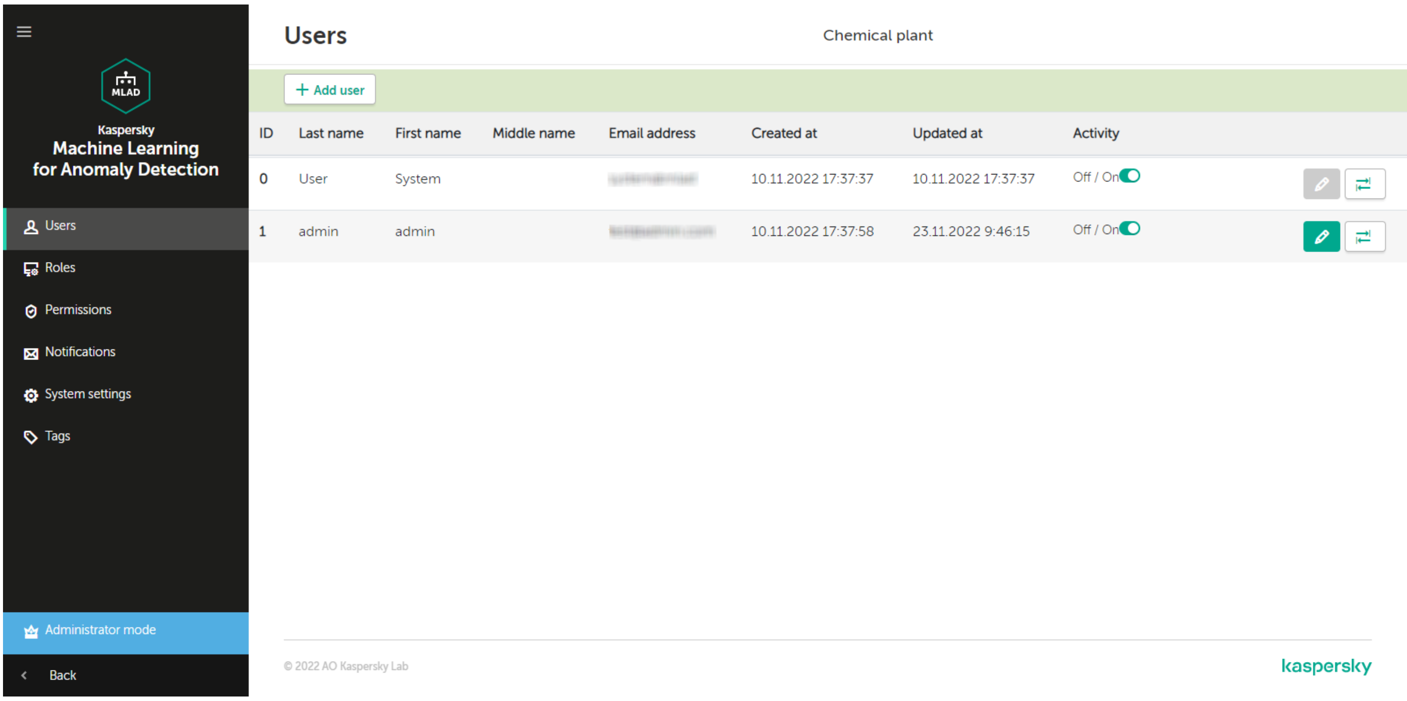
To ensure a safe user experience with Kaspersky MLAD, install a trusted certificate for connecting to the web interface, create an account for each user, configure and verify sending of incident messages to user emails.

All created user accounts are displayed under **Settings** → **Users**. The **Users** section contains a table that provides **information about users** ?.

- **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.
- **Created at** refers to the date and time when the user account was created.
- **Updated at** refers to the date and time when the user account was updated.
- **Activity** – toggle button allowing you to block or unblock a user account.

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 main settings of Kaspersky MLAD.

If necessary, you can also revoke keys for a user account.



ID	Last name	First name	Middle name	Email address	Created at	Updated at	Activity
0	User	System		[redacted]	10.11.2022 17:37:37	10.11.2022 17:37:37	Off / On
1	admin	admin		[redacted]	10.11.2022 17:37:58	23.11.2022 9:46:15	Off / On

Users section

Creating a user account

Kaspersky MLAD user accounts can be managed only by users that have administrator privileges.

To create a user account:

1. In the user menu, select the **Settings** section.

   The **Users** section opens.

2. Click the **Add user** button.

3. In the opened **Add user** window, fill in the following fields:

   - **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 (optional field).

   - **Email address** refers to the user's email address.

   - **Password** refers to the password for the user account.

     The password must consist of uppercase and lowercase English letters, and numbers. The minimum password length is eight characters.

   - **Confirm password** means you must type the password again to confirm the password for the user account.

4. Click the **Add** button.

Information about the new user will be displayed in the table. If necessary, you can edit, block or unblock user accounts.

The *Administrator* or *Operator* role cannot be assigned to a user while the user account is being created. You can assign the *Administrator* or *Operator* role to a user only when editing the user account.

Editing a user account

Kaspersky MLAD user accounts can be managed only by users that have administrator privileges.

To edit a user account:

1. In the user menu, select the **Settings** section.

   The **Users** section opens.

2. Click the edit button ✎ next to the user account that you want to edit.

   The **Edit user** window opens.

3. Make the necessary changes.

4. If necessary, assign the **Administrator** or **Operator** role to the user account by selecting the corresponding check box.

5. If you need to block or unblock a user account, turn on or turn off the **Activity** toggle button.

   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.

6. Click the **Save** button.

The updated information about the user will be displayed in the table.

Revoking keys for a user account

After a user connects to the Kaspersky MLAD web interface, an individualized key 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 devices, a key is created for each user session. If necessary, you can revoke keys for a user account at any time. For the user whose keys are revoked, their work session in the application will be closed simultaneously on all devices on which they were authorized. Revoking keys may be useful if you need to immediately terminate application connection sessions for a specific user.

To revoke a key or keys for a user account:

1. In the user menu, select the **Settings** section.

   The **Users** section opens.

2. Click the key revocation button ⇄ next to the user account whose keys you want to revoke.

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

The user account keys will be revoked, and the user session will be terminated.

Blocking and unblocking user accounts

You can 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 keys for the user account expired.
- An administrator has revoked keys for the user account.

To block or unblock a user account:

1. In the user menu, select the **Settings** section.

   The **Users** section opens.

2. Do one of the following for the relevant user:

   - To block a user account, turn off the **Activity** toggle button in the relevant row of the table.
   - To unblock a user account, turn on the **Activity** toggle button in the relevant row of the table.

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.

Incident notifications can be managed only by users with administrator privileges.

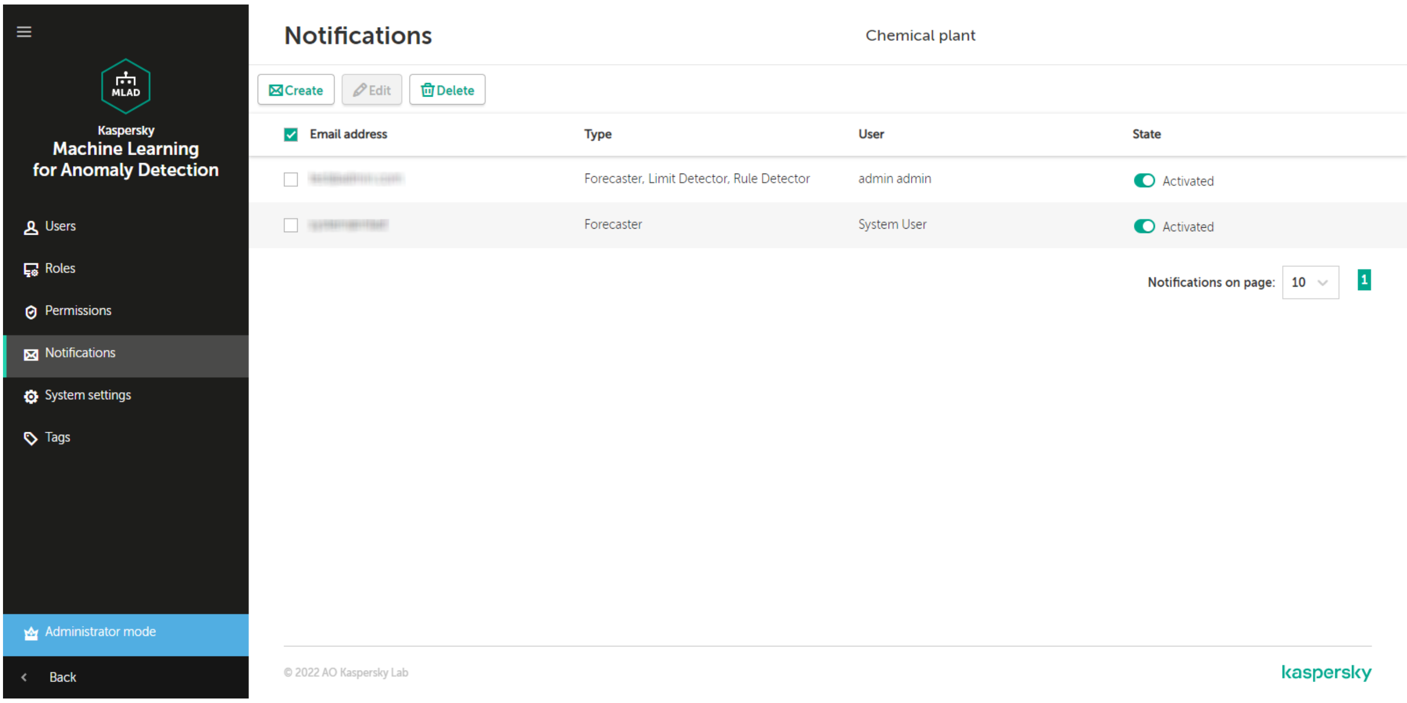
The Mail Notifier service must be configured and started in advance.

All generated incident notifications are displayed under **Settings** → **Notifications**. The **Notifications** section contains a table that provides **information about notifications**.

- **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

Chemical plant

☑ Email address	Type	User	State
□ [redacted]	Forecaster, Limit Detector, Rule Detector	admin admin	Activated
□ [redacted]	Forecaster	System User	Activated

Notifications on page: 10 1

© 2022 AO Kaspersky Lab

Notifications section

Creating an incident notification

Incident notifications can be managed only by users with administrator privileges.

To create an incident notification for a user:

1. In the user menu, select **Settings** → **Notifications**.

   You will switch to administrator mode.

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

   The **Create notification** window opens.

3. 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.

4. 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.

5. Specify the types of incidents for which you want to receive 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 set limit, select the **Limit Detector** check box.
   - If you want to configure a notification about an indicator tag value 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.

6. 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.

7. To enable sending of notifications, switch the **State** toggle button to the **Activated** position.

8. Click the **Create** button.

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

Editing an incident notification

Incident notifications can be managed only by users with administrator privileges.

To edit an incident notification:

1. In the user menu, select **Settings** → **Notifications**.

   You will switch to administrator mode.

2. 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.

3. Make the necessary changes.

4. If necessary, enable or disable sending incident notifications using the **State** toggle button.

5. Click the **Edit** 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

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 forwarding of notifications at any time.

To enable or disable sending of incident notifications:

1. In the user menu, select **Settings** → **Notifications**.

   You will switch to administrator mode.

2. Use the toggle button in the **State** column to enable or disable sending of the desired incident notification.

Deleting an incident notification

Incident notifications can be managed only by users with administrator privileges.

To delete an incident notification:

1. In the user menu, select **Settings** → **Notifications**.

   You will switch to administrator mode.

2. 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.

3. 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.

Removing the application

Removal of Kaspersky MLAD must be performed by an administrator (Kaspersky employee or 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.

To remove Kaspersky MLAD:

1. Go to the folder where Kaspersky MLAD is installed (mlad-release-3.0.0-<installation build number> by default).

   ```
   cd mlad-release-3.0.0-<build number>
   ```

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

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

3. Confirm removal of Kaspersky MLAD components.

Kaspersky MLAD will be removed.

Connecting to Kaspersky MLAD and closing the session

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

When a user connects, the application generates a key that is valid for seven days. During this time, the application does not prompt for user account credentials, provided that the connection is used by the same computer, browser, and user account. When the key expires, the application automatically closes the connection session for the user.

To terminate a connection session before the key expires, an authorized user can log out of the account manually. If necessary, a user with administrator permissions can also revoke the account keys from the user. When the user's keys are revoked, their work sessions in the application are terminated simultaneously on all devices on which they are authorized.

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

3. On the account credential entry page that opens, enter your login and password.

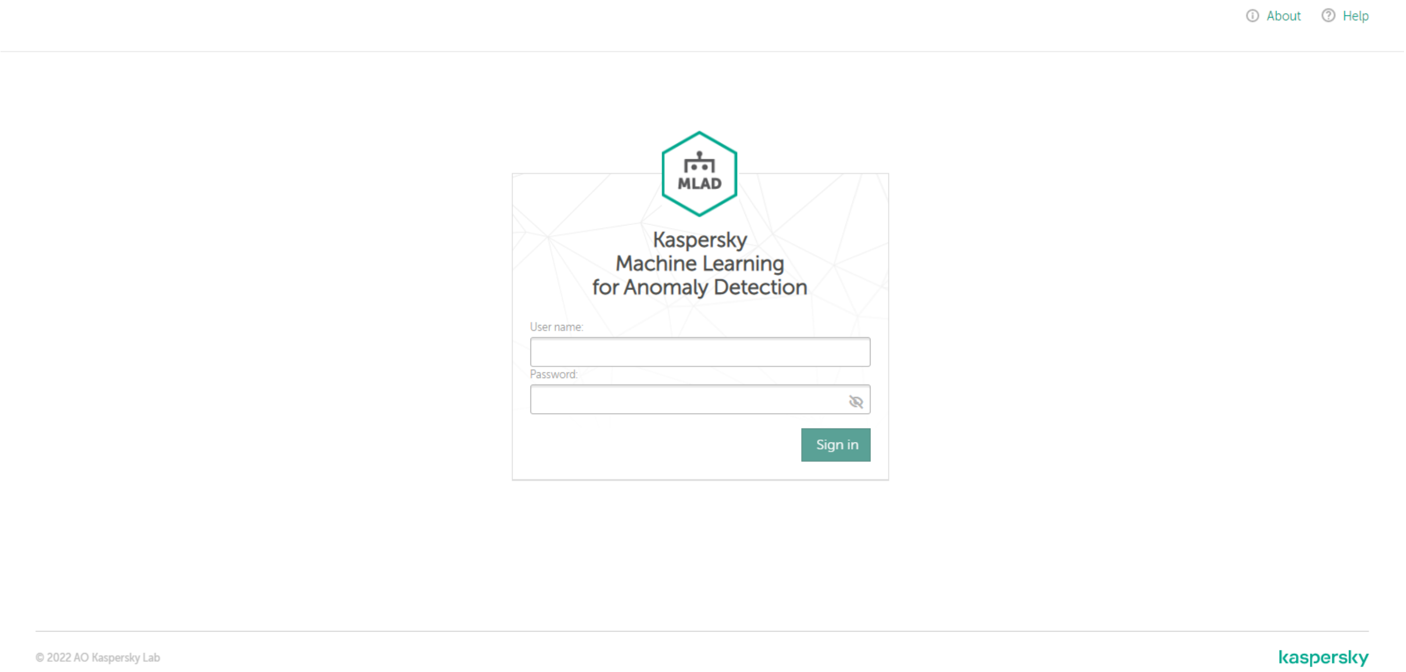
   When connecting to Kaspersky MLAD web interface for the first time, use the default login and password.

4. Click the **Sign in** button or press **ENTER**.

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

If you close the browser window without terminating the connection session, the session remains active. An application connection session that is not properly closed remains active for seven days. During this time, the application continues to grant access to the Kaspersky MLAD web interface page without prompting for user account credentials, provided that the connection is used by the same computer, browser, and operating system user account.

> In case of unsuccessful authorization, if the number of unsuccessful authorization attempts is reached, Kaspersky MLAD blocks your account for the specified period. The number of unsuccessful authorization attempts and the account blocking period can be specified by a user with administrator rights when the main Kaspersky MLAD settings are configured.



Page for entering the account credentials for Kaspersky MLAD

Closing a Kaspersky MLAD connection session

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

To close the connection session:

In the browser window on the Kaspersky MLAD web interface page, open the user menu and select **Sign out**.

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

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:

- Menu in the left part of the application web interface window
- Workspace in the central part of the application web interface window

The menu consists of a main menu and a user menu, which can be opened by clicking ◉ in the lower-left corner of the page. If necessary, you can also collapse or expand the main menu by clicking ≡ in the upper-left corner of the page.

Users with administrator privileges can access a menu that allows to manage user accounts, configure incident notifications, manage tags, and proceed to the logging system page to view logs.

Main menu

The main menu of Kaspersky MLAD includes the following sections:

▦	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.	⚙	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.		

User menu

The Kaspersky MLAD user menu includes the following elements:

English / Russian Lets you select the localization language for the Kaspersky MLAD web interface. It is available in English and Russian.	**Sign out** Signing out of the current user account.
Settings Opens the administrator menu where you can manage user account credentials, view user roles and permissions, configure incident notifications, and manage tags. The administrator menu is available only for users with administrator privileges.	**Logging** Takes you to the logging system (Grafana™) in a new browser tab. This section is available only to users with administrator privileges.
Help Opens the Kaspersky MLAD Help Guide in a new browser tab.	**About** Opens the page containing brief information about the application.

Administrator menu

The Kaspersky MLAD administrator menu is available only to users with administrator permissions and includes the following sections:

👤	Users Opens the section in which you can manage user accounts.	🖥	Roles Opens the section containing information about available user roles.
🛡	Permissions 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 components.	🏷	Tags Opens the section in which you can manage tags.
‹	**Back** Exits administrator mode and switches to the **Dashboard** section.		

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 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 installation of the application. If you do not accept the terms of the End User License Agreement, you must stop the installation of the application and must 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.

A license entitles you to the following types of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Technical Support

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.

Processing and storing data in Kaspersky MLAD

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

About data provision

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

The application does not send users' personal data to Kaspersky. Users' personal data is processed on the computers on which the application is installed.

The application processes and saves the following data related to users' personal data:

- Names of user accounts
- User names for connecting through the web interface
- Email addresses of incident notification recipients
- IP addresses or names of computers that were used to connect to the application web interface

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

The last names, first names, middle names and email addresses of application users are saved in plaintext. The confidentiality of this data must be ensured by a qualified application administrator employed by the Customer.

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 administrator. The application 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 application does not monitor access to the application installation settings file, which may contain personal data. The application monitors startups of application components that involve scanning user account credentials.

> The logging system (Grafana) does not transmit personal user data to Kaspersky or to third-party servers. Data may be sent to third-party servers based on user activity. Before starting to work with the logging system, it is recommended to read the Grafana User Guide.

Any received information is protected by Kaspersky in accordance with legally established requirements and applicable regulations of Kaspersky. Data is transmitted over encrypted communication channels.

Folders for storing application data

Kaspersky MLAD uses the following folders and subfolders for storing data:

- Application directories (by default, mlad-release-3.0.0-<installation build number>):

  - . – 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 – folder for storing data that is loaded using the HTTP Connector.
  - ./containers – folder for storing an archive of containers for Kaspersky MLAD services. Containers of Kaspersky MLAD services are installed to Docker from this archive.
  - ./legal – folder for storing the text of the End User License Agreement and the date of its acceptance by the user.
  - ./ssl – folder for storing the script for generating a self-signed certificate that provides an HTTPS connection to the Kaspersky MLAD user's browser.
  - ./ssl/tokens – folder for storing a JWT (JSON Web Token) key.
  - ./ssl/nginx – folder for storing certificates supporting an HTTPS connection with the browser of the Kaspersky MLAD user.
  - ./upgrade_backup-<version number>-<build number> – folder 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.
  - ./volumes_backup_<date of deletion> – folder for storing backup copies of Docker volumes that are created during removal of Kaspersky MLAD.
- Folder /var/lib/docker/volumes/:
  - ./mlad-release-<version number>-<installation build number>_postgres-volume – folder for storing Postgres database files.
  - ./mlad-release-<version number>-<installation build number>_inflxdb-volume – folder for storing Time Series Database files.
  - ./mlad-release-<version number>-<installation build number>_logger-volume – folder for storing the logging subsystem files.
  - ./mlad-release-<version number>-<installation build number>_webstatic-volume – folder 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 a user with application administrator privileges 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.

Performing common tasks

This section contains a description of the common user tasks and instructions on how to perform them.

Scenario: Working with Kaspersky MLAD

This section describes the actions of users having operator permissions when working with 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, the results of their processing by Kaspersky MLAD, and the generated predictions and identified incidents. 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**

   Go to the **Event Processor** section and view the events and patterns detected by the Event Processor. 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.
  - **Top tag** refers to the name of a technological process parameter for which the incident is registered.
  - **Detector** is the name of the detector that registered the incident.

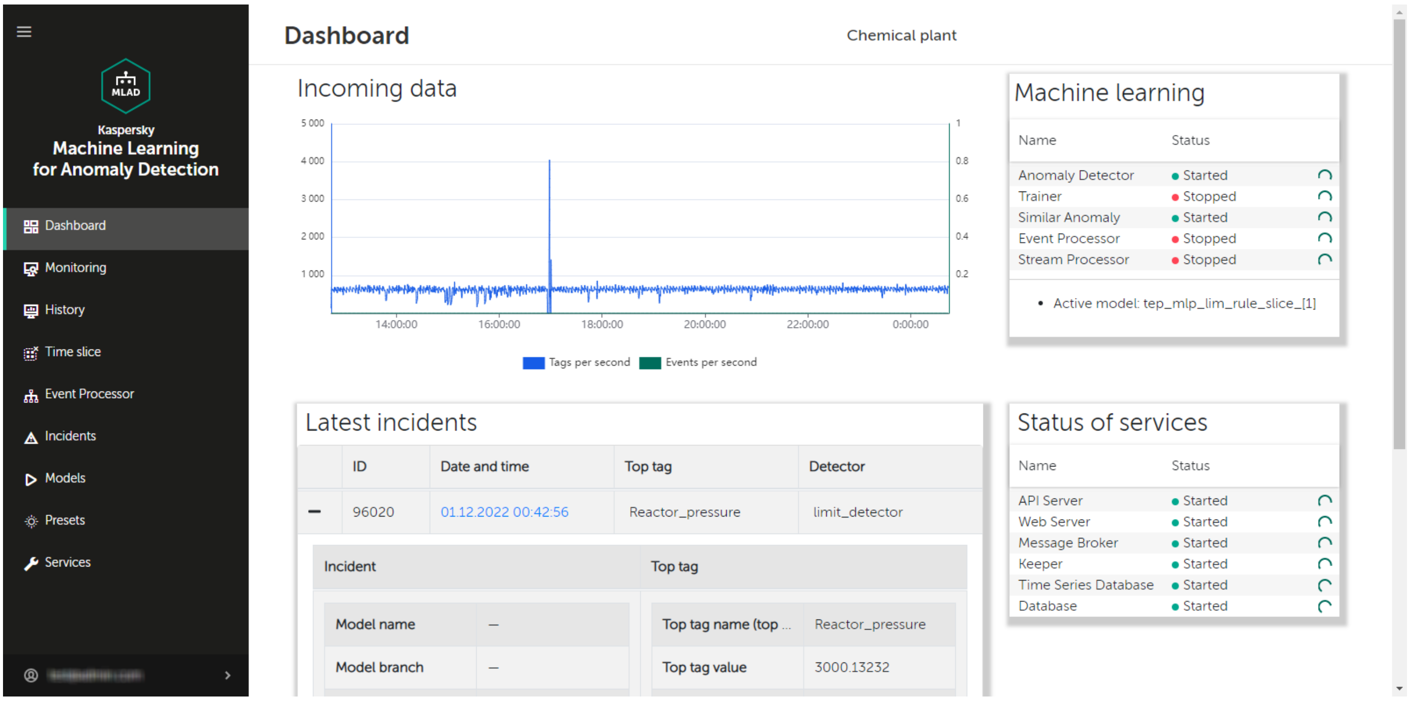
  Clicking the plus (+) next to the incident in the incidents table opens a window with the technical specification of the selected incident and tag:

  - **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 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.
    - **Limits** refer to the acceptable limits of values for a top tag.
    - **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.



Machine learning

Name	Status
Anomaly Detector	● Started
Trainer	● Stopped
Similar Anomaly	● Started
Event Processor	● Stopped
Stream Processor	● Stopped

- Active model: tep_mlp_lim_rule_slice_[1]

Latest incidents

	ID	Date and time	Top tag	Detector
−	96020	01.12.2022 00:42:56	Reactor_pressure	limit_detector

Incident		Top tag	
Model name	–	Top tag name (top ...	Reactor_pressure
Model branch	–	Top tag value	3000.13232

Status of services

Name	Status
API Server	● Started
Web Server	● Started
Message Broker	● Started
Keeper	● Started
Time Series Database	● Started
Database	● Started

Dashboard section

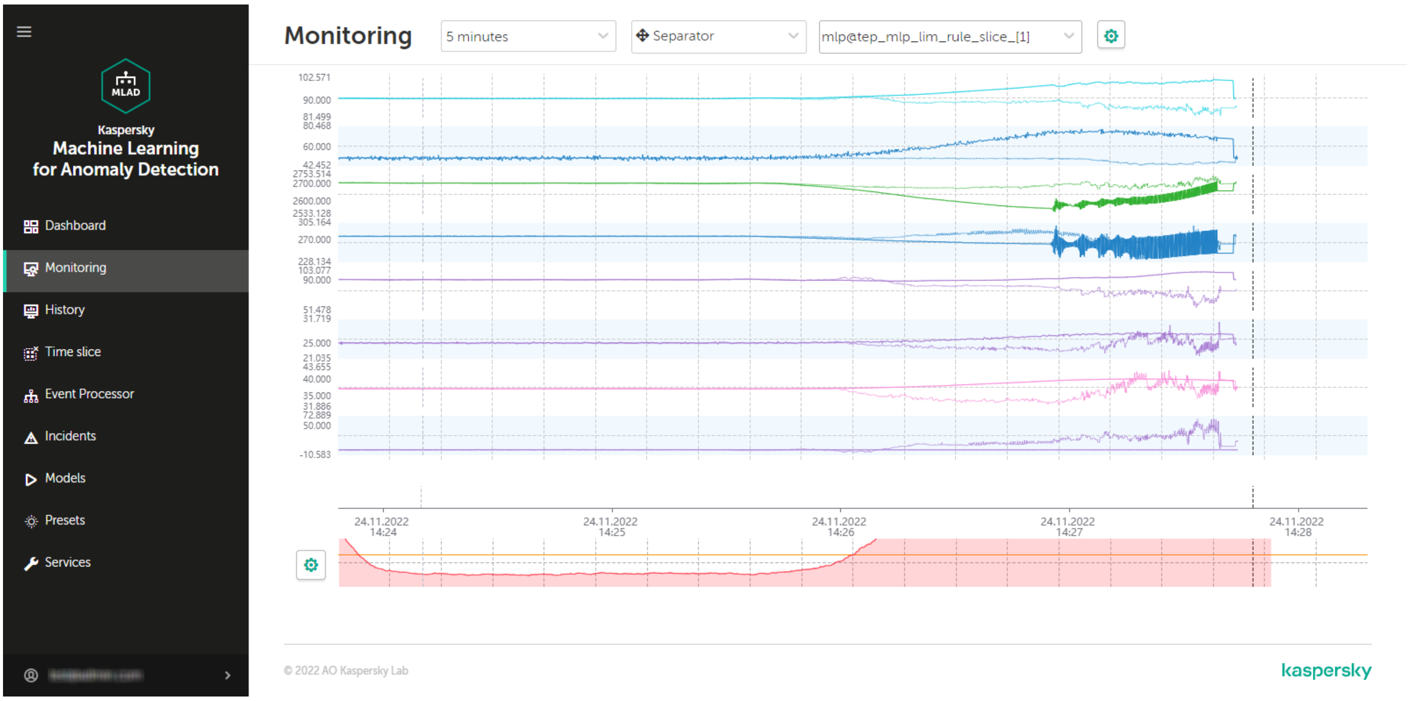
Viewing incoming data in the Monitoring section

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 of indicator tags for 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.

Incidents registered by the Rule Detector will not have an MSE value because incident registration occurs when an indicator tag value equal to one is reached. 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 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 indicator tags 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 of indicator tags for 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 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 of indicator tags 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, a user with administrator privileges can create, edit, or delete the 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 graphs in selected color** toggle button to enable the display of tag graphs in a specific color and select the color.
6. If necessary, move the **Predicted tag value** toggle button to enable the display of the predicted tag value and values of indicator tags of diagnostic rules on graphs.
7. If you need the graphs to display the defined technical limits for a tag:
   1. Turn on the **Technical limits** toggle button.
   2. If you need to always display the defined technical limits, turn on the **Always show technical limits** toggle button.

      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.
8. If necessary, move the **Personal tag error** toggle button to enable display of the personal tag error on graphs.
9. If necessary, move the **Tag description and name** toggle button to enable display of the tag description and name on graphs.
10. If necessary, move the **Additional threshold lines** toggle button to enable the display of additional threshold lines on the graph.

11. If necessary, move the **Display indicators for all incidents** toggle button 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.

12. 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.

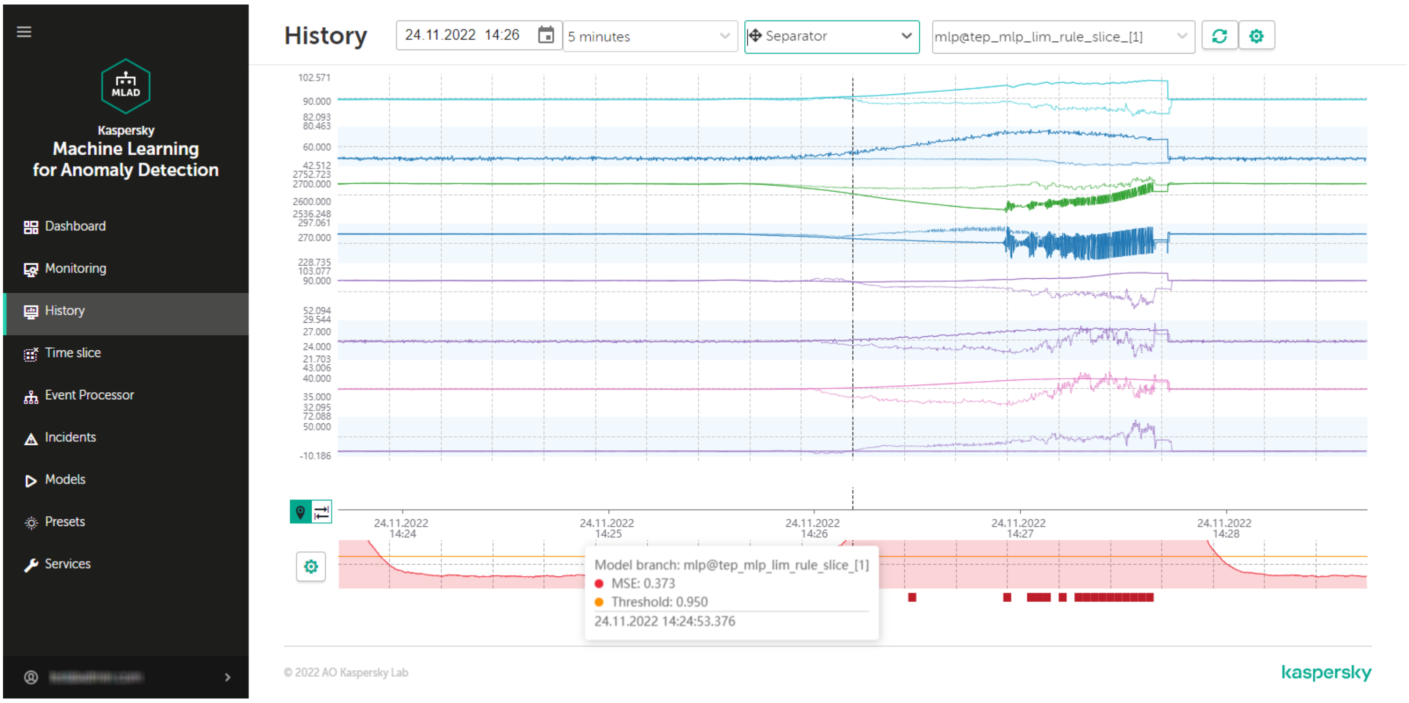
Viewing data in the History section

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 of indicator tags for 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.

Incidents registered by the Rule Detector will not have an MSE value because incident registration occurs when an indicator tag value equal to one is reached. 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.



Model branch: mlp@tep_mlp_lim_rule_slice_[1]
- ● MSE: 0.373
- ● Threshold: 0.950

24.11.2022 14:24:53.376

History section

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 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 indicator tags 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 of indicator tags for 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 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 of indicator tags 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, a user with administrator privileges can create, edit, or delete the 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.

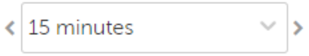
Navigating through time in the History section

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, move the **Show graphs in selected color** toggle button to enable the display of tag graphs in a specific color and select the color.

5. If necessary, move the **Predicted tag value** toggle button to enable the display of the predicted tag value and values of indicator tags of diagnostic rules on graphs.

6. If you need the graphs to display the defined technical limits for a tag:

   a. Turn on the **Technical limits** toggle button.

   b. If you need to always display the defined technical limits, turn on the **Always show technical limits** toggle button.

      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.

7. If necessary, move the **Personal tag error** toggle button to enable display of the personal tag error on graphs.

8. If necessary, move the **Tag description and name** toggle button to enable display of the tag description and name on graphs.

9. If necessary, move the **Additional threshold lines** toggle button to enable the display of additional threshold lines on the graph.

10. If necessary, move the **Display indicators for all incidents** toggle button 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. 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

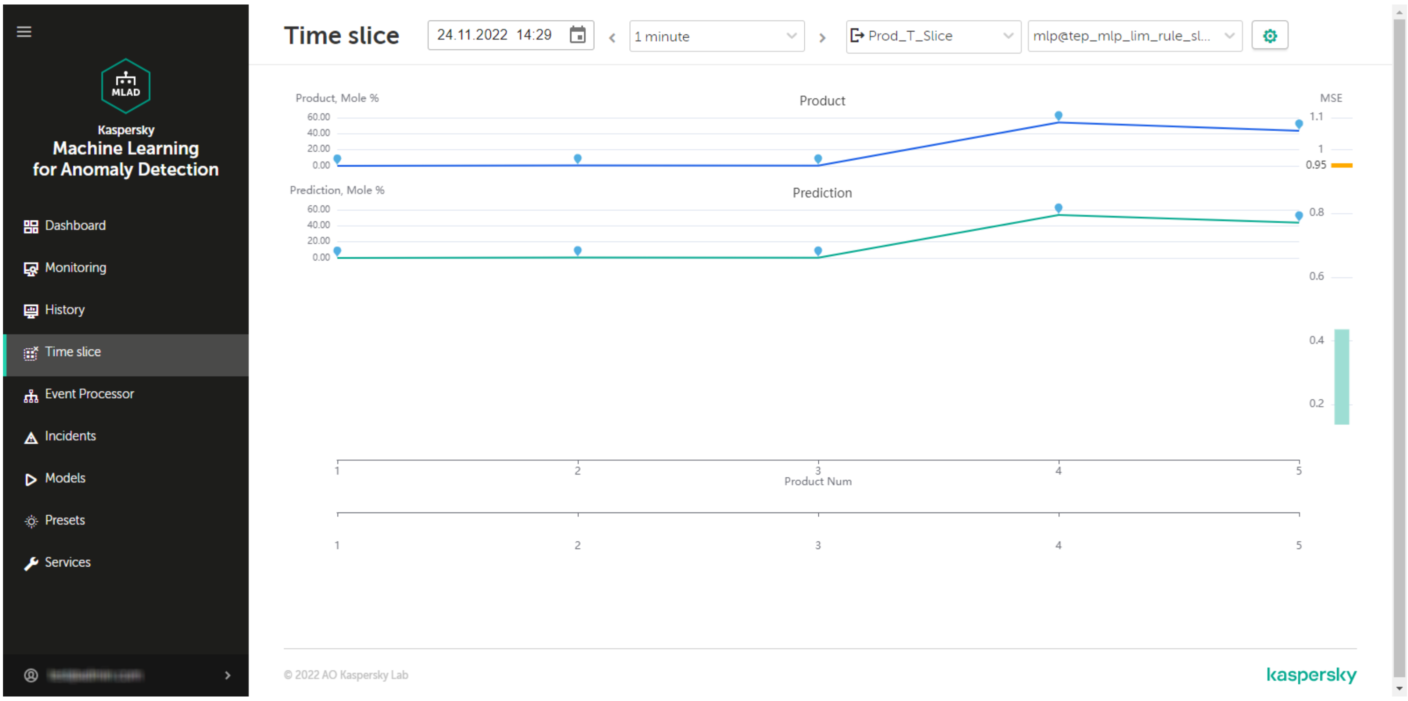
In the **Time slice** section, you can view the values of process parameters received from sensors of the monitored asset at the same point in time. The sensors must be of the same type (have the same dimension) and must be positioned linearly, like pressure sensors in an oil pipeline, for example.

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 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, a user with administrator privileges can create, edit, or delete the 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.

‹ 15 minutes ›

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.

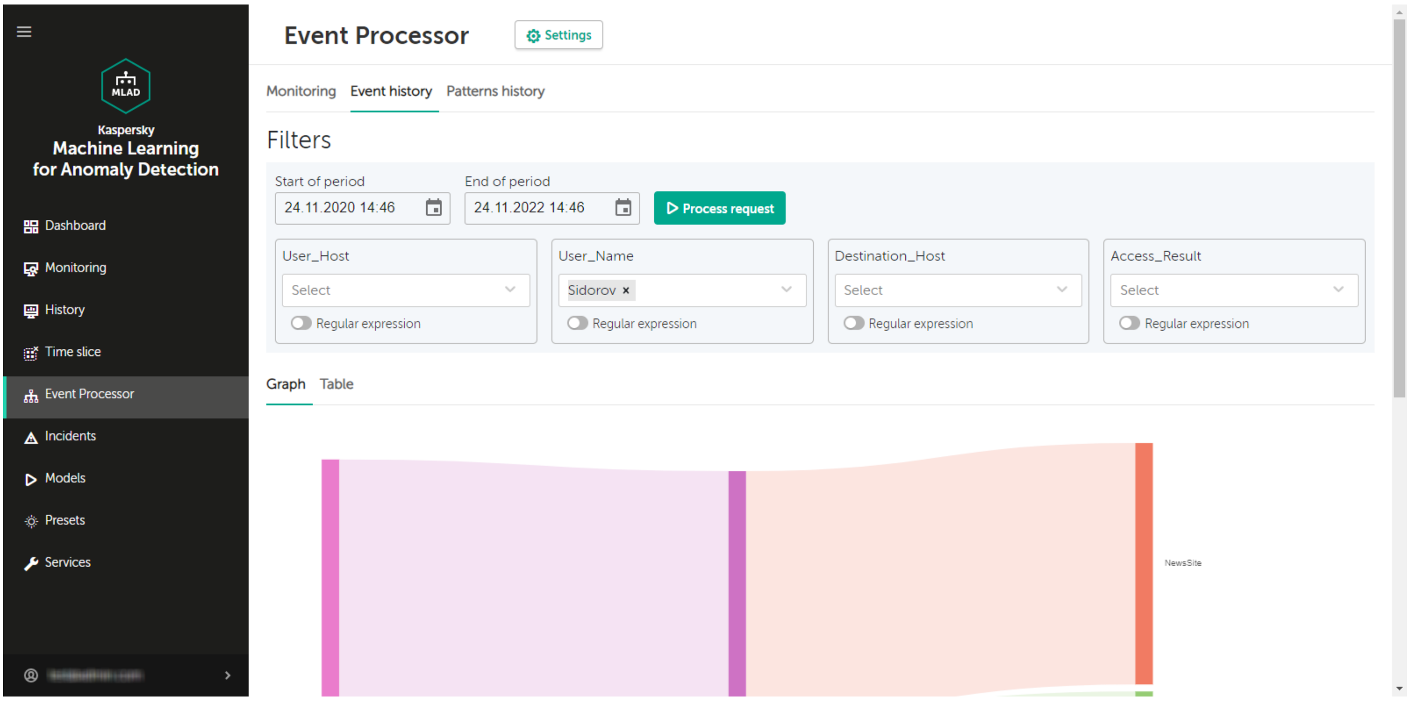
   The configured graph display settings will be applied.

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 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: 24.11.2020 14:46

End of period: 24.11.2022 14:46

User_Host: Select ○ Regular expression

User_Name: Sidorov × ○ Regular expression

Destination_Host: Select ○ Regular expression

Access_Result: Select ○ Regular expression

Event Processor section

Working with monitors

In the **Event Processor** section on the **Monitoring** tab, 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 an administrator (Kaspersky expert or 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

To create a monitor:

1. In the main menu, select the **Event Processor** section.

2. On the opened page, select the **Monitoring** tab.

3. Click the **Create monitor** button.

   The **Create monitor** pane appears on the right.

4. Specify the monitor name in the **Name** field.

5. 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.

6. 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.

7. In the **Stack limit** field, specify the number of monitor activations that must be displayed when viewing information about the monitor.

8. 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**.

9. If you need to track new events, patterns, or values of event parameters, turn on the **Only new** toggle button in the **Filters** section.

10. 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.

11. 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 button 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.

12. Click the **Create** button.

The new monitor is created and displayed on the **Monitoring** tab.

Deleting a monitor

To delete a monitor:

1. In the main menu, select the **Event Processor** section.
2. On the opened page, select the **Monitoring** tab.
3. 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**.

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 an administrator (Kaspersky expert or certified integrator) during configuration of the Event Processor service.

To upload data for viewing incoming events:

1. In the main menu, select the **Event Processor** section.
2. On the opened page, select the **Event history** tab.

3. 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.

4. 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.

5. 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

On the **Patterns history** page, 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 settings by a user with administrator privileges.

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 Kaspersky expert or certified integrator during configuration of the Event Processor service.

To view the registered patterns:

1. In the main menu, select the **Event Processor** section.

2. On the opened page, select the **Patterns history** tab.

3. 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 button 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.

4. 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.

5. 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.

6. 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.

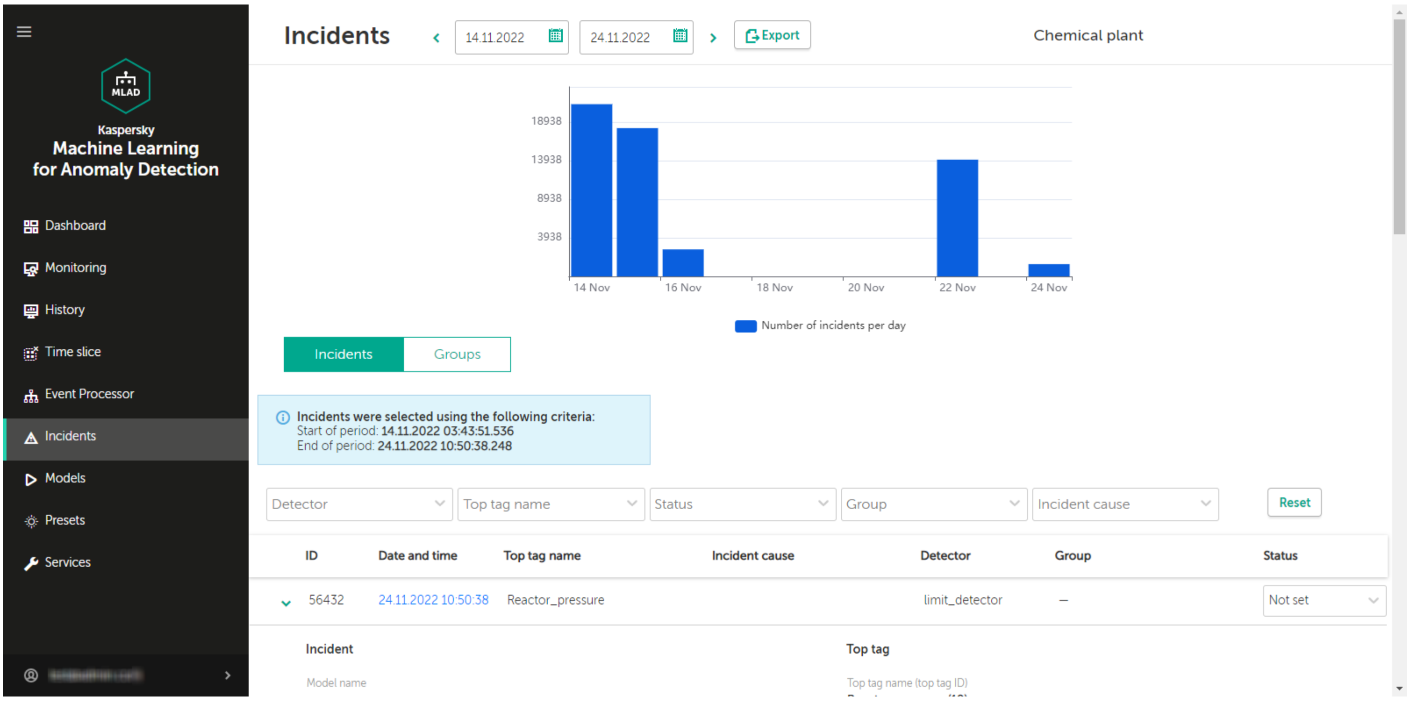
The graph can display up to 60 bars. If the specified period does not exceed 60 days, incidents on the graph are grouped by days. If the specified period is between 60 days and 60 weeks, incidents on the graph are grouped by weeks. If the specified period is longer than 60 weeks, incidents on the graph 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: 14.11.2022 03:43:51.536
End of period: 24.11.2022 10:50:38.248

ID	Date and time	Top tag name	Incident cause	Detector	Group	Status
56432	24.11.2022 10:50:38	Reactor_pressure		limit_detector	–	Not set

Incident
Model name

Top tag
Top tag name (top tag ID)

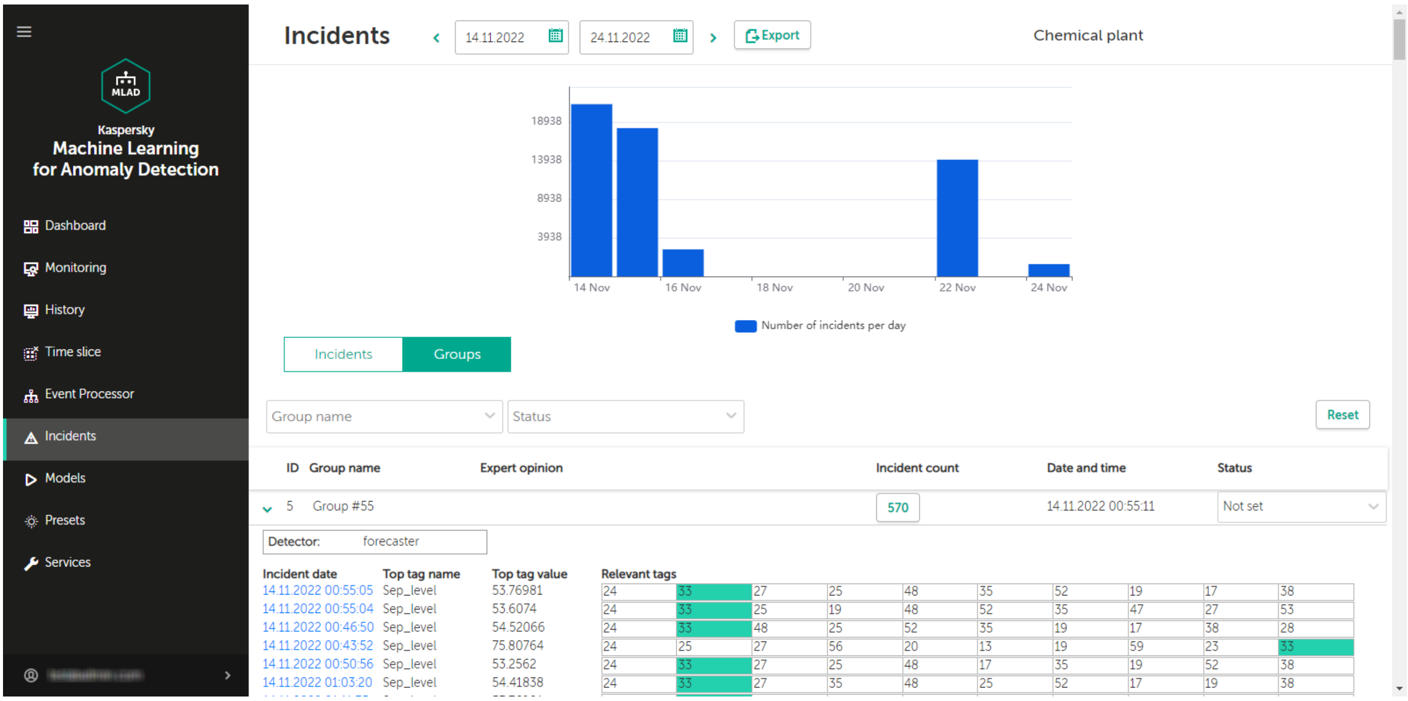
Incidents tab

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
5	Group #55		570	14.11.2022 00:55:11	Not set

Detector: forecaster

Incident date	Top tag name	Top tag value	Relevant tags									
14.11.2022 00:55:05	Sep_level	53.76981	24	33	27	25	48	35	52	19	17	38
14.11.2022 00:55:04	Sep_level	53.6074	24	33	25	19	48	52	35	47	27	53
14.11.2022 00:46:50	Sep_level	54.52066	24	33	48	25	52	35	19	17	38	28
14.11.2022 00:43:52	Sep_level	75.80764	24	25	27	56	20	13	19	59	23	33
14.11.2022 00:50:56	Sep_level	53.2562	24	33	27	25	48	17	35	19	52	38
14.11.2022 01:03:20	Sep_level	54.41838	24	33	27	35	48	25	52	17	19	38

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**. 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 that was registered by the Rule Detector, the application automatically creates the Tags for event #N preset, which contains the indicator tag that invoked registration of the incident.

- **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 the registered incident added by an expert (process engineer or ICS specialist) based on the results of the incident analysis.

- **Detector** refers to the name of the detector that identified an anomaly and registered the incident: Forecaster, Limit Detector, XGBoost, 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 component. 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 registered incident specified by an expert (process engineer or ICS specialist) based on the results of the incident analysis.

  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, a user with administrator privileges can create, edit, or delete the 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, XGBoost, 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 an indicator tag for the diagnostic rule. For the Limit Detector, the tag whose value exceeded the technical limits defined for this tag will be displayed.

  - **Top tag value** is the value of the top tag registered when the incident occurred.

  - **Limits** refer to the acceptable technical limits of values for a top tag.

  - **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, a user with administrator privileges 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 component). 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, a user with administrator privileges can create, edit, or delete the 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.

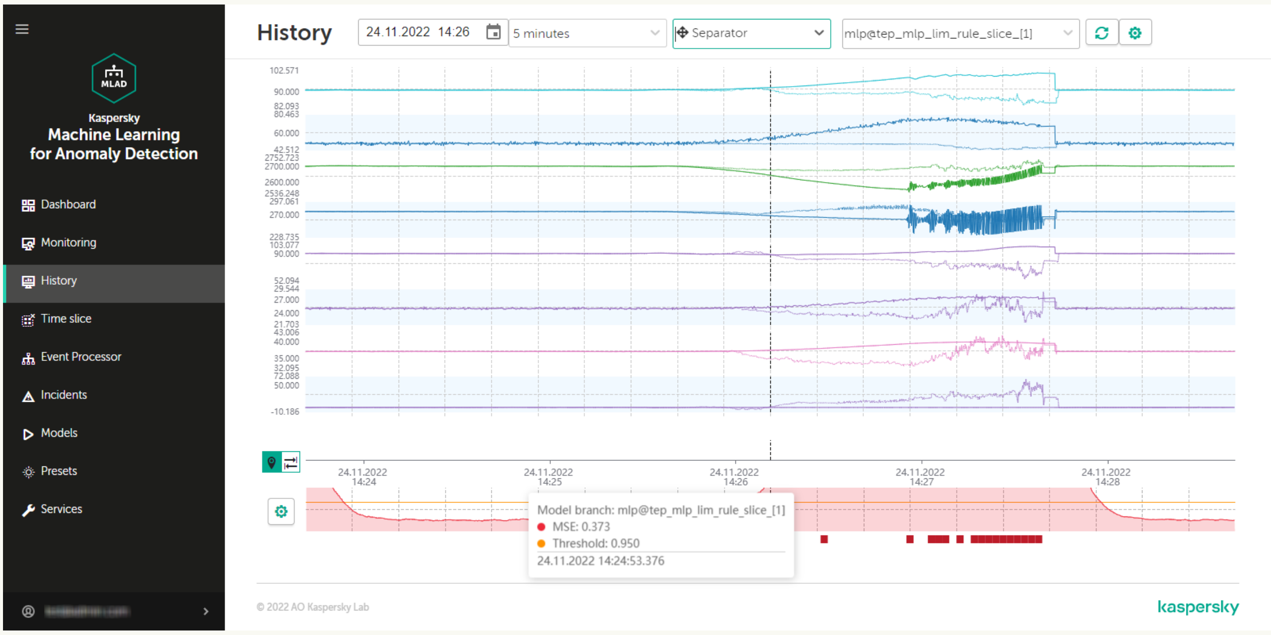
- The indicator tag of the triggered diagnostic rule and the tags included in this rule, if the incident was registered by the Rule Detector.

- The tag whose value was outside the limits of the permissible range of values, 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.



Model branch: mlp@tep_mlp_lim_rule_slice_[1]
● MSE: 0.373
● Threshold: 0.950
24.11.2022 14:24:53.376

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 the values of indicator tags showing the results from applying 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 (technical limits) are defined for a tag, enable the **Always show technical limits** 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 boundaries of the tag graph. If tag values go beyond the permissible limits, the vertical scale will be automatically changed to display the tag values exceeding the limits.

- 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 technical limits, even if the **Always show technical limits** 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, a user with administrator privileges can create, edit, or delete the 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, a user with administrator privileges 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, a user with administrator privileges can create, edit, or delete the 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 folder 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®.

Working with ML models and templates

The **Models** section provides data on ML models and on the templates created based on the ML models added to Kaspersky MLAD.

The **Models** tab displays a table of ML models uploaded to Kaspersky MLAD or added based on the templates by the users with administrator privileges. There is a vertical menu ⋮ next to each model in the table that allows you to view detailed information about the model. You can view information about the ML model parameters and parameters of ML model elements, as well as view the diagram of the data flow between ML model elements.

The **Templates** tab provides a table of templates created by the users with administrator privileges based on ML models added to Kaspersky MLAD.

Viewing ML model parameters

To view the parameters of an ML model:

1. In the main menu, select the **Models** section.
2. Click the vertical menu ⋮ next to the ML model whose data you need to view.
3. To view the ML model parameters, select **Model details**.

   The **<ML model name>** pane opens on the right on the **Model parameters** tab displaying a list of ML model parameters.

An ML model is characterized by the following parameters:

- **ID** – automatically assigned short identifier of the ML model.
- **Model name** – name of the ML model. The parameter can be changed by users with administrator privileges.
- **UUID** – automatically assigned full identifier of the ML model.
- **Description** – description of the ML model. The parameter can be changed by users with administrator privileges.
- **File name** – name of the ML model file.
- **Version** – version of the ML model.
- **Updated by** – name of the user who performed the last update of the ML model.
- **Updated at** – date and time of the last update of the ML model.
- **Created by** – name of the user who created the ML model.
- **Created at** – date and time when the ML model was created.

Viewing ML model element parameters

To view the parameters of an ML model element:

1. In the main menu, select the **Models** section.
2. Click the vertical menu ⋮ next to the ML model whose data you need to view, and select **Model details**.

The **<ML model name>** pane opens on the right showing detailed information on the ML model.

3. To view the parameters of an ML model element, select the **Model elements** tab and click the down arrow (⌄) next to the relevant ML model element.

   The **<Model name>** pane displays a list of the ML model element.parameters.

A list of ML model element parameters and their descriptions are provided in the table below.

ML model element parameters

ML model element parameters	Description of ML model element parameters
ID	Automatically assigned short identifier of the ML model element.
Element name	Name of the ML model element. This parameter can be edited.
UUID	Automatically assigned full identifier of the ML model element.
element_path	Path to the ML model element.
block_type	Type of ML model element (for example, *neural_forecaster* – predictive neural network or *rule*).
color	Color to display the ML model element and indicator points of the incidents registered by the ML model element on the graphs in the **Monitoring** and **History** sections. This parameter can be edited.
alpha	Parameter for smoothing the cumulative MSE (for an ML model based on the Forecaster detector) or parameter for smoothing the anomaly detection probability (for a model based on the XGBoost detector). This parameter can be edited.
delta_t	Parameter that determines the step of the time grid (in nanoseconds). The ML model works with data calculated on a uniform temporal grid. Conversion of the received telemetry data to a uniform temporal grid is performed automatically.
tag_ids	List of tag identifiers included in the ML model element. Details on the tag_ids parameter. This list of tags is used for selecting the input tags (the **in_tags** parameter) to provide the initial data for prediction, and the output tags (the **out_tags** parameter) whose values are predicted by the ML model element. The sets of tags in the **in_tags** and **out_tags** parameters can overlap or coincide. The ML model does not necessarily analyze all the available tags of the monitored asset. If the ML model is based on the Rule Detector, output tags whose values are predicted by the ML model element may include special indicator tags signaling that a rule was triggered. The particular selection of tags is made by an expert when creating an ML model.
in_tags	List of tags that serve as input data for predicting the values of the output tags (**out_tags**).
indicator_tags	List of output indicator tags included in the ML model element. This parameter is available only in the list of parameters of the ML model based on the Rule Detector.
input_window_size	Input interval of observations measured by the number of steps of the time grid (size of the input window). Details on the input_window_size parameter.

	This parameter determines the size of the input values window for the **in_tags** parameters of the ML model element. They are used by this ML model element to determine the output values of the **out_tags** parameters in the output window **forecast_window_size**: • Predicted for the Forecaster detector. • Calculated for the Rule Detector. • Predicted with a certain probability for the XGBoost detector. The window size is defined as the number of **delta_t** intervals.
power	Power indicator of the cumulative forecast error (MSE). This parameter can be edited and is available only in the list of parameters of the ML model based on the Forecaster detector.
threshold	Threshold value for an incident registration. This parameter is available only in the list of parameters of the ML model based on the Forecaster detector. Details on the threshold parameter. The threshold parameter is interpreted as follows: • For a model based on the Forecaster detector, this parameter refers to the threshold of the cumulative MSE and can be edited. • For a model based on the XGBoost detector, this parameter refers to the probability value limit that results in anomaly detection when exceeded. • For indicator tags based on the Rule Detector, the threshold value is always considered equal to one.
batch_size	Number of input windows processed by the ML model element in one pass during training. This parameter is available only in the list of parameters of the ML model based on the Forecaster detector.
forecast_shift	Offset of the forecast window **forecast_window_size** relative to the start of the input window **input_window_size** (in time grid steps).
forecast_window_size	Size of the output window for which the ML model element determines the values of the output tags **out_tags** based on the input tags **in_tags** in the input window **input_window_size**. The output window size is specified as the number of time grid steps.
out_tags and mse_weights	List of output tags and their relative weights. The values of output tags are predicted by the ML model and then compared with the actual values. This parameter can be edited and is available only in the list of parameters of the ML model based on the Forecaster detector. Details on the out_tags and mse_weights parameters.

	It is characterized by the following constituent elements: • **Tag ID** is the ID of the output tag. If the ML model is based on the Rule Detector, the identifier of an output tag may contain indicator tags for each rule included in the model element. • **Tag name** is the name of the output tag. • **Weight value** is the weight of the prediction error of the output tag value in the cumulative MSE. The sum of the weights of all output tags is automatically normalized to one.
mode	MSE calculating method used by the Anomaly Detector service. This parameter is available only in the list of parameters of the ML model based on the Forecaster detector. Details on the mode parameter. The **mode** parameter supports the following MSE calculating methods: • **REAL** – MSE is calculated every time the real tag values change. • **REAL_DECIMATED** – MSE is calculated when the actual tag values change, but not more than once per every time grid step **delta_t**. • **UNIFORM** – MSE is calculated at the nodes of the uniform temporal grid with the **delta_t** step. • **ALL** – MSE is calculated at the nodes of the uniform temporal grid with the **delta_t** step, as well as every time the real tag values change. • **ALL_DECIMATED** – MSE is calculated at the nodes of the uniform temporal grid with the **delta_t** step, as well as when the actual tag values change, but not more frequently than once per **delta_t** step. If telemetry data is converted to a uniform temporal grid by the Stream Processor service before being transmitted to the ML model for processing, the MSE value is the same regardless of the selected MSE calculation method.

In neural network ML models, the cumulative prediction error denoted by the MSE parameter in the application web interface is usually calculated with exponential smoothing, as the sum of the instantaneous prediction errors at the current and previous points, and the contribution of a point lagging k steps behind decreases with the coefficient (1-**alpha**)^k. The cumulative error is calculated as the **power**-th root of the **mse_weights**-weighted sum of the individual instantaneous prediction errors for each output tag to the specified **power**. The MSE value is calculated without smoothing when the **alpha** parameter is set to `1`.

Viewing the data flow diagram of an ML model

You can view a diagram showing how data flows between elements of an ML model.

To view the data flow diagram of an ML model:

1. In the main menu, select the **Models** section.

2. Click the vertical menu ⋮ next to the ML model whose data you need to view, and select **Model details**.

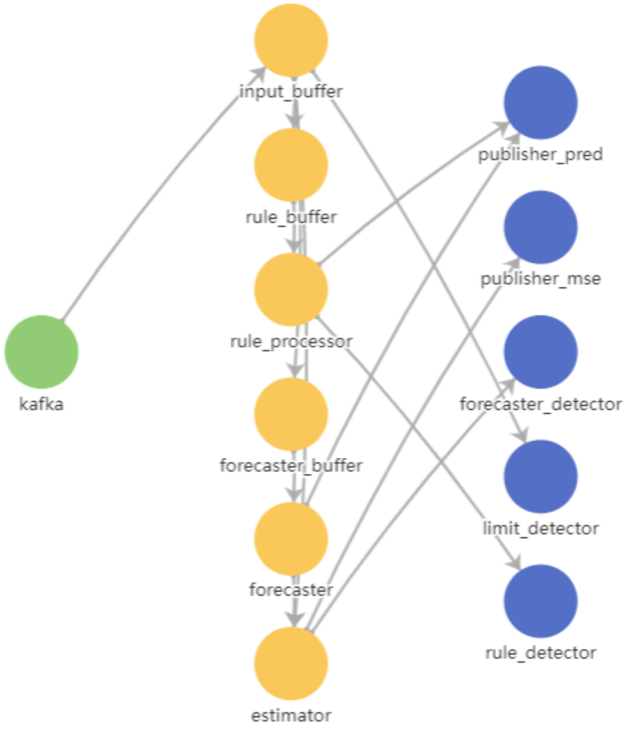
   The **<ML model name>** pane opens on the right showing detailed information on the ML model.

3. Select the **Data flow diagram** tab.

   The **<ML model name>** pane displays a diagram of the data flow between ML model elements.

4. If you need to view the settings of an ML model element, move the mouse cursor over it.

   A window listing the values of settings of the selected element will be displayed.



ML model data flow diagram

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.

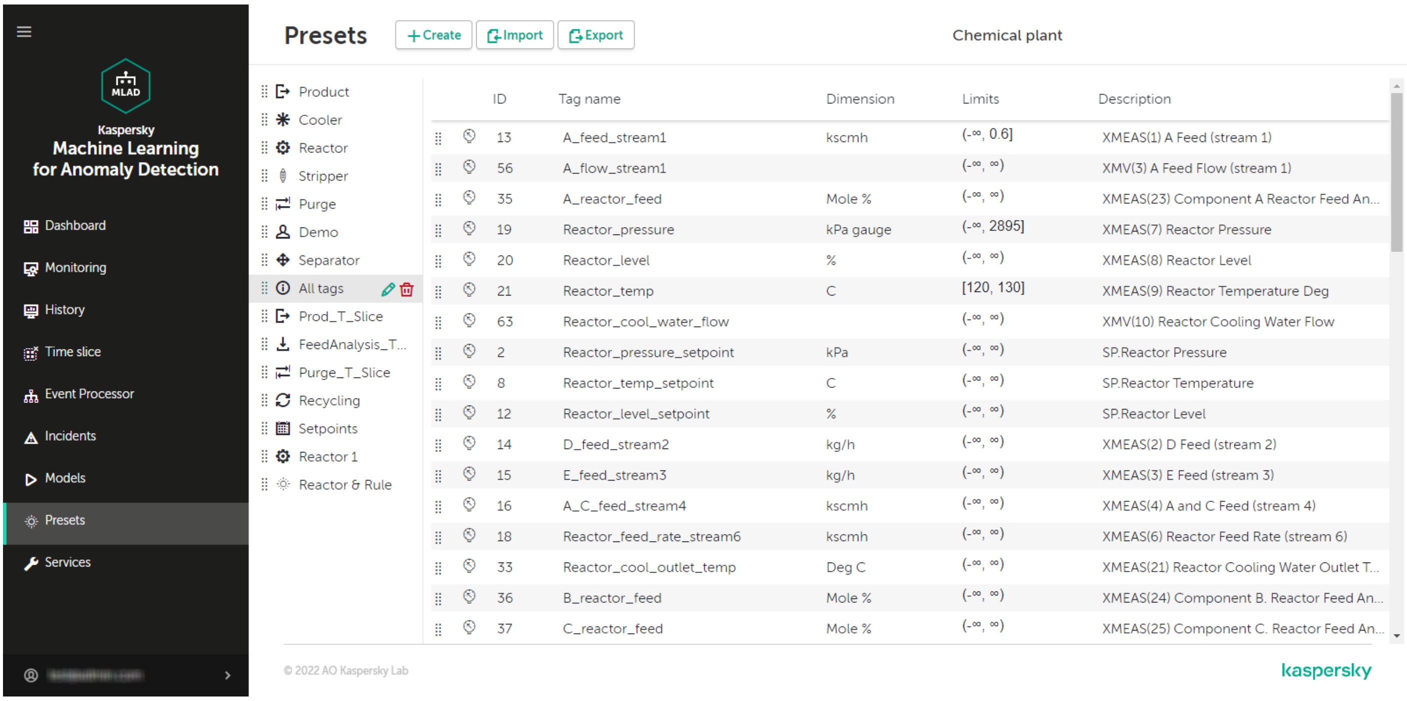
To view the received data on the graphs in the **History** and **Monitoring** sections, upload the preset configuration to Kaspersky MLAD from a JSON file. As part of Kaspersky MLAD deployment, a common preset configuration can be created for all users.

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.



ID	Tag name	Dimension	Limits	Description
13	A_feed_stream1	kscmh	(-∞, 0.6]	XMEAS(1) A Feed (stream 1)
56	A_flow_stream1		(-∞, ∞)	XMV(3) A Feed Flow (stream 1)
35	A_reactor_feed	Mole %	(-∞, ∞)	XMEAS(23) Component A Reactor Feed An...
19	Reactor_pressure	kPa gauge	(-∞, 2895]	XMEAS(7) Reactor Pressure
20	Reactor_level	%	(-∞, ∞)	XMEAS(8) Reactor Level
21	Reactor_temp	C	[120, 130]	XMEAS(9) Reactor Temperature Deg
63	Reactor_cool_water_flow		(-∞, ∞)	XMV(10) Reactor Cooling Water Flow
2	Reactor_pressure_setpoint	kPa	(-∞, ∞)	SP.Reactor Pressure
8	Reactor_temp_setpoint	C	(-∞, ∞)	SP.Reactor Temperature
12	Reactor_level_setpoint	%	(-∞, ∞)	SP.Reactor Level
14	D_feed_stream2	kg/h	(-∞, ∞)	XMEAS(2) D Feed (stream 2)
15	E_feed_stream3	kg/h	(-∞, ∞)	XMEAS(3) E Feed (stream 3)
16	A_C_feed_stream4	kscmh	(-∞, ∞)	XMEAS(4) A and C Feed (stream 4)
18	Reactor_feed_rate_stream6	kscmh	(-∞, ∞)	XMEAS(6) Reactor Feed Rate (stream 6)
33	Reactor_cool_outlet_temp	Deg C	(-∞, ∞)	XMEAS(21) Reactor Cooling Water Outlet T...
36	B_reactor_feed	Mole %	(-∞, ∞)	XMEAS(24) Component B. Reactor Feed An...
37	C_reactor_feed	Mole %	(-∞, ∞)	XMEAS(25) Component C. Reactor Feed An...

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.
   - **Limits** refers to the limit values for the tag; when these values 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 you need to change the preset icon, click the **Choose an icon** button and select the appropriate icon 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 button.

   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 list 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 list of tags.

8. Click the **Create** 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 tag 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 an 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 button.

   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. If the file is uploaded by a user with administrator privileges, the tag configuration is uploaded to the application as well.

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.

Viewing the status of a service

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). Only a user with administrator privileges can start, stop, or restart Kaspersky MLAD services.

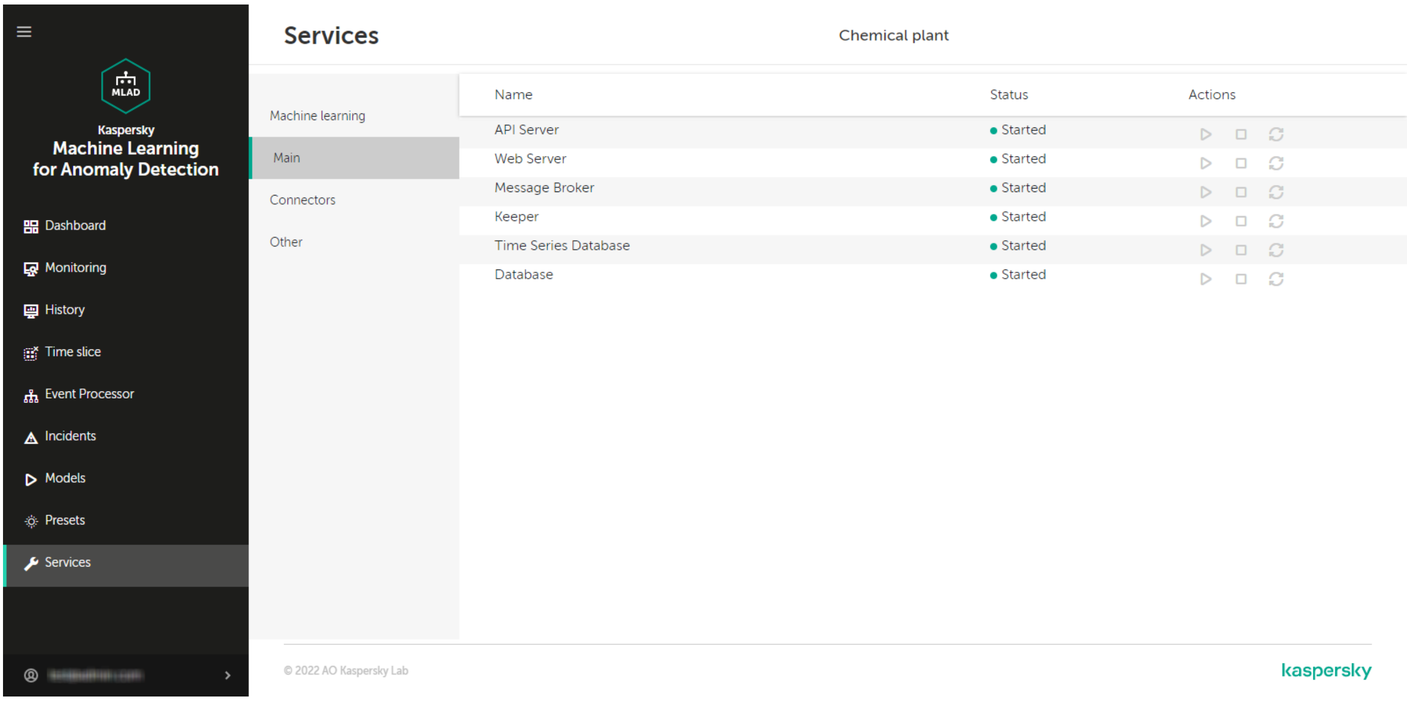
You can view the status of a service to make sure that the service was successfully started or stopped.

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).



Name	Status	Actions
API Server	● Started	▷ □ ↻
Web Server	● Started	▷ □ ↻
Message Broker	● Started	▷ □ ↻
Keeper	● Started	▷ □ ↻
Time Series Database	● Started	▷ □ ↻
Database	● Started	▷ □ ↻

Services section

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, contact a qualified administrator – a Customer employee who has the right to accept the application License Agreement. The administrator 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, perform the following steps:
   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** 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** 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 specified by the administrator.

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.

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 browser address bar, enter the Kaspersky MLAD web address received from the ICS specialist.

3. On the account credentials entry page that opens, click **Help** (?).

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.

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 Kaspersky Lab employee or 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 the CEF Connector to an external source of events.
CEF_INCOMING_PORT	Port number that will be used to connect the CEF Connector to an external source of events.

To apply changes to the configuration file, restart Kaspersky MLAD.

Example JSON file containing a tag configuration

Below is an example of a JSON file containing descriptions of tags, their configuration, and presets.

A user with administrator privileges uploads the tag configuration in the **Settings** → **Tags** section. The configuration of the presets described in the JSON file is also uploaded to Kaspersky MLAD. A user with operator privileges can upload only preset configurations.

```
{
 "tags": {
 "1": {
 "id": 1,
 "name": "Sep_level_setpoint",
 "description": "Separator-level setpoint",
 "tag_type": "",
 "measurement_units": "%",
 "plc_id": "TEP",
 "real_type": "line",
 "predicted_type": "spline",
 "max": null,
 "min": null,
 "high_limit": null,
 "low_limit": null,
 "cls": "level",
 "type": "SV",
 "position": [],
 "icon": null,
 "expressions": null,
 "is_virtual": false,
"bias": 0,
"multiplier": 1,
"threshold_lines": null
},
...
"121": {
"id": 121,
"name": "No reactor temperature response",
"description": "Rule",
"tag_type": "13",
"measurement_units": "",
"plc_id": "",
"real_type": "line",
"predicted_type": "spline",
"max": null,
"min": null,
"high_limit": null,
"low_limit": null,
"cls": "level",
"type": "PV",
"position": [],
"icon": null,
"expressions": null,
"is_virtual": false,
"bias": 0,
"multiplier": 1,
"threshold_lines": null
}
},
"tags_structure": [
{
"directory_id": "root",
"name": "Root",
"description": null,
"children": [
"tags",
"trash_bin"
],
"icon": null
},
...
{
"directory_id": "tags",
"name": "Chemical plant",
"description": null,
"children": [
"Reactor",
"Separator",
"Stripper",
"Product",
"Purge",
"Cooler",
"a5eeb30739a742d3955765608ff73229"
],
"icon": null
}
],
"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"
 }
 ],
 "version": 2
}
```

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.

The configuration file is created by a Kaspersky expert or a certified integrator. A user with administrator privileges 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": "count",
 "tooltip": {
 "templates": [
 "{{User_Name}} » {{User_Host}}",
 "Count: {{count}}"
 ]
 },
 "isGraphGroup": true
 }, {
 "source": "User_Host",
 "target": "Destination_Host",
 "value": "count",
 "tooltip": {
 "templates": [
 "{{User_Host}} » {{Destination_Host}}",
 "DeviceEventClassID: {{Access_Result}}",
 "Count: {{count}}"
 ]
 }
 }
 ]
}
```

Viewing the Kaspersky MLAD log

The Kaspersky MLAD log stores entries only for the last 48 hours.

Naming 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 folder>-<image name>-#,
```

where # is the number of the Docker container.

By default, Kaspersky MLAD uses the `mlad-release-3.0.0-<installation build number>` folder.

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-3.0.0-<installation build number>-anomaly_detector-1
Time Series Database	influxdb	mlad-release-3.0.0-<installation build number>-influxdb-1
Message Broker	kafka	mlad-release-3.0.0-<installation build number>-kafka-1
Keeper	keeper	mlad-release-3.0.0-<installation build number>-keeper-1
Logger	logger	mlad-release-3.0.0-<installation build number>-logger-1
Database	postgres	mlad-release-3.0.0-<installation build number>-postgres-1
Similar Anomaly	similar_anomaly	mlad-release-3.0.0-<installation build number>-similar_anomaly-1
Event Processor	event-processor	mlad-release-3.0.0-<installation build number>-event-processor-1
Stream Processor	stream-processor	mlad-release-3.0.0-<installation build number>-stream-processor-1
Trainer	trainer	mlad-release-3.0.0-<installation build number>-trainer-1
Web Server	nginx-ui	mlad-release-3.0.0-<installation build number>-nginx-ui-1
API Server	web-server	mlad-release-3.0.0-<installation build number>-web-server-1
Mail Notifier	postman	mlad-release-3.0.0-<installation build number>-postman-1
OPC UA Connector	opcua-connector	mlad-release-3.0.0-<installation build number>-opcua-connector-1
MQTT Connector	mqtt-connector	mlad-release-3.0.0-<installation build number>-mqtt-connector-1
AMQP Connector	amqp-connector	mlad-release-3.0.0-<installation build number>-amqp-connector-1
HTTP Connector	gate	mlad-release-3.0.0-<installation build number>-gate-1

KICS Connector	kics3-connector	mlad-release-3.0.0-<installation build number>-kics3-connector-1
CEF Connector	cef-connector	mlad-release-3.0.0-<installation build number>-cef-connector-1
WebSocket Connector	ws-connector	mlad-release-3.0.0-<installation build number>-ws-connector-1
	webstatic	mlad-release-3.0.0-<installation build number>-webstatic-1
	migrations	mlad-release-3.0.0-<installation build number>-migrations-1

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**

   Select the **Logging** section from the user menu. This opens the Grafana interface in which you need to enter the login and password of the Kaspersky MLAD user.

   This is available only for Kaspersky MLAD users with the administrator role.

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 metrics and logs

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**

   Select the **Logging** subsection from the user menu. This opens the Grafana interface in which you need to enter the login and password of the Kaspersky MLAD user.

   This is available only for Kaspersky MLAD users with the administrator role.

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 form.

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`.

Glossary

Account role

Set of access rights that determine the actions available to a user when connected to the application web interface. There are two roles available to users in Kaspersky MLAD: Administrator and Operator.

Anomaly

Any deviation in the behavior of a monitored asset that is abnormal, unexpected, and not prescribed by the industrial process.

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.

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.

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.

Notification

A message with information about an incident (or incidents), which is sent by the application via notification delivery systems (for example, via 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.

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 folder (in the 'legal' subfolder).

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Ubuntu is a registered trademark 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.

Microsoft and Excel are trademarks of Microsoft Corporation.

Python is a trademark or registered trademark of Python Software Foundation.