kaspersky

Extended Technical Support Program Security Account Manager for Kaspersky Anti Targeted Attack

SAM for KATA

kaspersky

1. General terms and conditions

Herein is given a list of technical support cases, in relation to which Kaspersky will provide assistance to the owner of certificate of Security Account Manager for Kaspersky Anti Targeted Attack platform (hereinafter referred to as SAM for KATA).

This SAM for KATA Support Program is aimed at providing the End User with technical support of enhanced quality, as compared to the terms of standard Technical Support carried out in accordance with the Kaspersky End User License Agreement, which determines the terms of utilizing the software Product by the End User.

2. Definitions

"Company Account" shall mean web-based Kaspersky Technical Support request processing system

"Product(s)" shall mean software product(s) of Kaspersky, which the Customer has purchased, deployed and installed in accordance with the terms of a License Agreement between Kaspersky and the Customer, and for which the Customer has concluded a License Agreement.

"End User", **"User"**, **"Customer", (You / Your)** shall mean an organization, which has a functioning license to the Product that is supported in accordance with to this Program.

"Incident" shall mean any event reported by the Customer, which is not part of the standard operation of a Product and which causes, or may cause, an interruption to, or a reduction in, the quality of service provided by the Product.

"Local Time" shall mean the time zone of the Kaspersky Local Office

"Problem" shall mean an unknown underlying cause of one or more Incidents. It becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

"Known Error" shall mean a Problem that becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

"Product Error" shall mean undeclared behavior of the Product.

"Service Request" shall mean a request from a Customer for support, delivery, information, advice or documentation, which is not related to an incorrect functioning or non-functioning of the Product(s).

"Virus Outbreak" shall mean a Customer crisis situation, where a virus undetected by the Product(s) with the latest antivirus bases and executable modules is affecting business continuity and/or a large number of Customer's end- users. Virus Outbreak is a product-related Incident.

"Malware-related Incident / Virus Incident" shall mean not product-related Incident, requiring Kaspersky to provide recommendations on particular malware removal, and/or malware descriptions, and/or special malware removal tools.

"Incident Severity/Urgency" shall mean a measure of the business criticality of an incident or problem based on the business needs of the Customer. See Appendix for more details.

"Response time" shall mean the elapsed time measured from the moment of any incident receipt till qualified answer to the initiator (via support system, email or phone).

"Update" shall mean Kaspersky-issued anti-virus databases with new virus signatures or modification of the Product's executable modules, which enhances its performance and/or expands its functionality.

"Upgrade" shall mean a Product update associated with assigning a new version number.

"Workaround" shall mean a procedure that may serve as a temporary solution to an incident.

"False Alarm", **"False Positive"** shall mean a situation when the Product erroneously detects a safe file as an infected one.

kaspersky

3. Description of SAM for KATA support program

Technical Support channels.

Technical support relating to product operations as well as acceptance of post- incident maintenance requests are implemented by the means of:

- Kaspersky Technical Support web portal with acceptance of requests 24 hours a day, 365 days a year
- Priority telephone line, depending on the urgency:
    - for Severity Level 1 and Severity Level 2 requests, 24 hours a day, 365 days a year;
    - for requests of levels 3–4, business hours of the Kaspersky Local Office.
- Email (only when having issues accessing Company Account), acceptance of requests 24 hours a day, 365 days a year
- Dedicated Security Account Manager, during business hours, local time

Incident processing

Processing incidents via Company Account web panel

Web-based Kaspersky Technical Support request processing system is available at: https://companyaccount.kaspersky.com

By the means of this system, Customer can take advantage of:

- access to personal account in order to create, update and monitor incidents;
- technical support and consulting in relation to incidents that may occur during Product installation, configuration and functioning;
- general consultations in relation to security incidents identified by customer after clarification of the event provided the Product.

Processing incidents by phone

Technical Support by phone is only available to the authorized contact persons of the Customer.

Processing incidents by email

Processing incidents by email can be used in the case of issues accessing the web Company Account. It is available to all authorized contact persons of the Customer.

Incident resolution control

At any moment, an incident can be either on the Customer's side (i.e. Customer is taking actions that will promote/expedite the resolution of the issue by Kaspersky) or on Kaspersky side.

An incident is on the Customer's side when Kaspersky requests information from the Customer. When Customer provides the requested information to Kaspersky, the Incident is considered to be on the side of the latter. The period during which the incident may be on the Customer's side, is limited to 1 month. In case the Customer's response is overdue, the incident is closed by timeout.

Kaspersky is only responsible for the time during which the incident is on their side.

kaspersky

Response times

Kaspersky guarantees the following response times, depending on the urgency of customer's request:

Severity level	Response time
Level 1	30 minutes*
Level 2	4 hours*
Level 3	6 working hours
Level 4	8 working hours

*Phone call is required during out of business hours incl. weekends and holidays

Requests from the customers of the SAM for KATA are assigned with higher priority compared to requests within the standard support package.

The urgency level is determined by the category chosen by the customer (using the drop down list in the Company Account) when contacting Technical Support and the gist of the incident. Kaspersky reserves the right to revise the request's urgency level if the severity of the case as specified by the customer is not confirmed. The list of urgency levels with descriptions is provided in the Appendix.

Dedicated Security Account Manager (SAM)

Security Account Manager (SAM) is assigned by Kaspersky with the purpose of maintaining an integrated channel of communication with the customer.

SAM is an employee of Kaspersky who manages processing of all the customer incidents. The responsibilities of Security Account Manager are determined as follows:

- organizing communication for processing incidents by Kaspersky technical teams;
- notifying Customer of the current status of incidents; providing regular reports;
- supervising the progress of tasks related to Customer requests and implementing timely escalations when processing requests for technical support requests;
- support Customer awareness about new Kaspersky security solutions portfolio;
- consulting Customer regarding Kaspersky Anti Targeted Attack platform functioning and assistance in responding to security incidents identified by customer by validating events provided by Kaspersky Anti Targeted Attack platform
- supervises the progress and coordinates work of team providing Incident response services (if service is purchases by the Customer)

SAM is accessible during business working hours local time by landline phone, by cellular phone and by email. If the SAM is unavailable (Outside of normal business hours including weekends), the Customer's requests are directed to the manager-on-duty on the MSA Technical Support line.

Business working hours may vary depending on the region, check Your SAM Service certificate for details.

Customer assigns contact persons (in accordance to Section 4) for communication with Kaspersky, and shares the list of their contact details (email, telephone number and others if available) for consistent and efficient collaboration in connection with incident resolution.

kaspersky

Quality management

Incident escalation and claim management

Reclamations concerning quality of technical support are accepted according to the following scheme:

Escalation level	1	2	3
	Security Account Manager	Head of support team, Kaspersky Regional office	Business Account Manager (Business Contact)

Customer may escalate unresolved incidents in case it is currently on the Kaspersky side.

Provision of reports on open incidents

During the process of incident resolution, Kaspersky will make every effort for promptly provide Customer with information on open incidents' status, according to the following table.

Severity level	Report schedule
Level 1	By agreement, but not more often than once a day (by email or by phone)
Level 2	Within the regular reports
Level 3	
Level 4	

Anti-virus database release by customer's request on malware incident or false positive

In case of a false negative (when an infected file is identified by the Product as safe) or, oppositely, a false positive, on condition that the latest available anti-virus databases are utilized, Customer may request to make changes to anti-virus signatures of the Product. Kaspersky provides Customer with the update of the Product that will ensure correct detection of the file.

Kaspersky implements the following activities:

- Processing requests concerning anti-virus databases release (carried out by a dedicated group of specialists in a 24/7/365 mode)
- Release of high-priority (expedited) updates for the subscribers of the SAM for KATA.
- Informing Customer about the progress of their requests by the means of Security Account Manager.

Provision of the public and private patches

- Processing requests concerning the release of patches and private fixes (carried out by a group of engineers dedicated for Enterprise subscribers' requests)
- Informing Customer about the progress of their requests by the means of Security Account Manager

Kaspersky will apply commercially reasonable efforts to release a private program correction code (private patch). Codes of program correction are released according to the product support lifecycle break down of the Support Service Terms and Conditions (an up-to-date version is available at: https://support.kaspersky.com/support/rules#en_us).

The terms of using private program corrections are a subject of the License Agreement between Kaspersky and the Customer.

Additional terms of support

Customer can assign up to 8 (eight) contact persons authorized to initiate requests to Kaspersky Technical Support. A list of authorized contact persons should be defined in Kaspersky SAM for KATA certificate. To change a list of authorized contact persons Customer should send a written request via Company Account. Kaspersky will provide a Customer with an updated version of Kaspersky SAM for KATA certificate.

Customer can register unlimited number of incidents, during Kaspersky SAM for KATA certificate validity.

Some incidents may require reproduction on Kaspersky side with the purpose of testing and verifying a virus infection or a product error.

Customer should provide Kaspersky with all information necessary and specific software or hardware, which may be necessary for reproducing the condition under which the incident will re-occur and could be examined. This may be needed if Kaspersky does not have the necessary software or hardware available.

Kaspersky will endeavor to reproduce the incident as soon as all of the necessary information and software and/or hardware is provided.

If the incident could not be reproduced, Customer should grant to Kaspersky specialists supervised remote access to the malfunctioning system.

If the incident cannot be reproduced by either party, or Customer did not grant access to the network environment where the incident could be reproduced, or if it is detected that the incident's cause lies beyond the Product, the incident cannot be classified within this Support Program.

If the Customer owns Kaspersky Private Security Network (KPSN) license along with Kaspersky Anti Targeted Attack licenses this terms of SAM for KATA program will apply to both products.

Limitations of the extended technical support program SAM for KATA

Technical support covered by the SAM for KATA program shall not be implemented in case of the following incidents;

- incidents already resolved for the Customer (i.e. incident that occurred on one installed copy of the Product after the same incident had been resolved for another copy of the Product);
- troubleshooting of all issues similar or identical to already resolved issues (i.e. the incidents to which a previously produced solution can be applied without additional guidance from Kaspersky);
- incidents caused by Customer's hardware malfunction;
- incidents caused by software platform incompatibility (including, but not limited to beta software, new versions of service packs or additions, whose compatibility with the Product has not been confirmed by Kaspersky);
- incidents caused by installing and running third-party applications (including, but not limited to the list of unsupported or incompatible applications published in the documentation);
- incidents for which the Customer cannot provide accurate information, as reasonably requested by Kaspersky, in order to reproduce, investigate, and resolve the incident;
- incidents which arise as a result of neglect or incorrect use of Kaspersky instructions, which, if

properly used, would have obviously prevented the incident.

Request types not covered by SAM for KATA package include (but are not limited to) the following:

- Verification and prioritization of KATA application alerts;
- Performing security incident investigation (service available at additional fee);
- Performing security incidents remediation.

4. Appendix

Product incident severity levels

"Severity Level 1" (critical) shall mean a critical Product problem, which affects Customer's business continuity by interruptions in the Product's normal functioning and which causes the Product(s) or Operating System to crash, or which causes data loss, changing default settings to insecure values, or security issues, provided that there is no Workaround available.

The list of Product-related incidents, which refer to Severity Level 1, includes, but is not limited to, the following issues:

- all local network (or its critical part) is inoperative, which hampers or suspends core business processes.

"Severity Level 2" (high) shall mean a moderate issue which affects product functionality but does not cause data corruption/loss or software crash. Severity Level 1 is re-classified to Severity Level 2 when a workaround is available.

The list of Product-related incidents, which refer to Severity Level 2, includes, but is not limited to, the following issues:

- product malfunctions or does not function, but continuity of core business processes is not broken.

"Severity Level 3" (medium) shall mean a non-critical issue or service request, which does not affect Product's functionality.

The list of incidents, which refer to Severity Level 3, includes, but is not limited to, the following issues:

- product is partially out of service (malfunctions), but other applications utilized by the Customer are not involved.

"Severity Level 4" (minor) shall mean other non-critical issues or service requests. Al incidents that do not satisfy any of the above-listed criteria, refer to this severity level.

Virus incident severity levels

"Severity Level 1" (critical) shall mean virus outbreak, which affects Customer's business continuity by interruptions in the Product's normal functioning and which causes the Product(s) or Operating System(s) to crash, or which causes data loss, provided that there is no Workaround available.

The list of malware-related incidents, which refer to Severity Level 1, includes, but is not limited to, the following issues:

- all local network (or its critical part) is inoperative;
- virus outbreak;
- false positive for the files that refer to business-essential systems.

"Severity Level 2" (high) shall mean a moderate issue which affects product functionality but does not cause data corruption/loss or software crash. Severity Level 1 is re-classified to Severity Level 2 when a workaround is available.

The list of malware-related incidents, which refer to Severity Level 2, includes, but is not limited to, the following issues:

- infection of some non-critical network nodes;
- false positive for the files that do not refer to business-essential systems.

www.kaspersky.com/
www.securelist.com