Case Template for SaaS Security products
---

1. Device Information (Platform and Software version)
Product:
Software: (version of PAN-OS)

2. Provide the URL of the Dashboard of your SaaS Security API tenant.
(Tenant Name / Region)

3. Describe the Issue (What?):
If applicable, please include troubleshooting steps taken.

4. Purpose for opening case.
[] Workaround provision
[] Root cause analysis
[] Q&A

5. Date/time of occurrence (When?):

6. Frequency of the problem.
[] Once (First time)
[] Random interval. Please specify in detail.
[] Fixed interval. Please specify in detail.

7. Service/Application outage?
[] Yes
[] No

8. Currently recovered?
[] No, problem still occurring
[] Yes, please specify how the system recovered (e.g. Recovered itself)

9. If any, what changes were done prior to this problem?
[] Nothing
[] Activate SaaS Security API/Inline newly
[] Changed the configuration in the tenant or device
[] Changed the surrounding equipment(s). Please specify in detail.
[] Maintenance work (Hardware replacement, system shutdown, etc.)
[] Change of usage situation (Change in traffic pattern, change in number of users, etc.)
[] Other

10. How many users this problem is affected?
[] One user
[] Multiple (but not all) users
[] All users

11. What kind of SaaS Application is affected by the reported issue?

12. Provide URL of Assets and/or Policy Rules (as much as possible)

13. Can data / logs be gathered?
[] Yes, the device is remotely accessible.
[] Yes, from the production network but remote access is unavailable.
[] Yes, the problem is reproduced in the lab.
[] No

14. Lab replication done:
[] Yes, please specify the steps regardless of replicated or not.
[] No, please specify why?

15. Execution summary by Partner (Log analysis, Reproduction attempts, etc.)

16. Detailed explanation of the attached file(s). Please explain all of them.