# [SAE] Issue Escalation Format

**Updated Sep 2025**

When escalating an issue to SAE through a Zendesk ticket or any other channels, please use the format below to provide all relevant details.
We understand that it may not always be possible to complete every field,
but the more information you provide, the less unnecessary back-and-forth will be required,
and the faster we can expect a response from KHQ.

## 1. Device Model:

Specify the device (camera/NVR/etc.) model you are using. (Example: XNV-8083R, XRN-6410DB4)

## 2. Firmware Version / Software Version:

State the current firmware version installed on the device.
If the issue is related to a WiseAI or any other OpenPlatform app, specify its version.
If it is related to VMS or other Software, specify the version in use.
Also include the upgrade path (previous version ➔ current version) if the issue happened after the upgrade.

## 3. Issue Description:

Describe the problem in as much detail as possible. Include:

- ***Summary****:* A brief statement of the problem, and the reason for escalation
- **Expected vs. Actual Result** (including any error codes or error messages)
- **Occurrence**: when the issue happens (specific time, after a certain period of operation, under certain conditions, etc.).
- **Recent changes**: firmware upgrades, configuration changes, or network modifications prior to the issue
- **Relevant configuration details** if you think they are related.
- **Temporary workaround** (if any, e.g., reboot resolves the issue temporarily)
- **Additional materials such as related screenshots or video clips** are very helpful in understanding the exact issue.

## 4. Reproducibility & Steps to Reproduce:

- Is the issue consistent, intermittent, or triggered only under certain conditions?
- Provide the exact steps to reproduce the problem.
  (Step-by-step instructions help support engineers recreate the environment.)

## 5. Environment Details:

Summarise the operating environment related to the issue, such as

- Network setup (IP settings, NAT/firewall usage, bandwidth constraints, VLANs, etc.),
- Client software and versions (mobile app, VMS, etc.),
- Any other external systems involved
- Device timezone and customer's local timezone if they are different (for log analysis)
- Scope of impact (isolated device/site or multiple devices/sites)

## 6. Logs or Diagnostic Files (if available):

Attach relevant system logs, event logs, packet captures or network traces from the time the issue occurred.
These are invaluable for troubleshooting.

### 6-1. Camera/Encoder

Three different log types are available (access/system/event).
Please check these logs and share any entries that appear related to the issue.

### 6-2. NVR/Decoder

The CSLOG contains detailed records of events when the issue occurred.
Regarding the CSLOG download URL, refer to this link.
When sharing the CSLOG, please make sure to always include the following information:

- The CSLOG export password
- The exact time when the issue was reproduced

(i.e. the time window when the issue is expected to have been recorded in the CSLOG — at least down to the minute)

### 6-3. SSM

Share logs from SSM Core Server.
Refer to this link for details on SSM 2.x logs.

### 6-4. Genetec/Milestone Hanwha Plug-in

Share logs from the Hanwha Plug-in.
Refer to this link for details about Genetec/Milestone Hanwha Plug-in logs.

## 7. Screenshots / Screen Recording:

Provide screenshots or short recordings showing the error messages or abnormal behaviour, along with timestamps if possible.
Note: if the issue is only described in text, it is very difficult to make an accurate assessment.

## 8. Contact & Priority / Issue Impact / Severity (optional):

Include the customer's information and any deadlines or urgency so that the issue can be prioritised appropriately.