Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

Event Overflow

Updated 2 September 2026

What Event Overflow Does

Event Overflow is a platform-wide stability safeguard in GCXONE that automatically protects the system from being flooded by a malfunctioning or misconfigured device. Without this protection, a single noisy sensor could send thousands of alarms in minutes, potentially overloading the entire alarm processing infrastructure and impacting all customers on the platform.

Why It Matters

Without Event Overflow protection, a single noisy sensor could flood the entire platform — impacting not just one customer but every customer sharing the infrastructure. The threshold system ensures that one misconfigured device cannot take down alarm processing for everyone else.

How It Works

GCXONE — Device Level

GCXONE operates a platform-wide default to prevent resource exhaustion. The system monitors incoming alarms at the individual device/sensor level:

- Threshold: If a single device sends more than 25 alarms within any 5-minute window, the overflow threshold is breached.
- Alarm Type: The system generates an internal alarm type called event.overflow to record and signal the incident.
- Suppression: All further alarms from that specific sensor are discarded for the remainder of the 5-minute window.

- Recurrence: The system re-checks at the start of each new 5-minute window. If the alarm rate remains above the threshold, another event.overflow is raised and suppression continues.

Talos (CMS) — Site Level

Even if individual device alarm counts pass through GCXONE, they may still be blocked at the CMS (Evalink Talos) level, which applies overflow logic at the site level — across all devices on a site:

- Site-level threshold: Talos aggregates alarms across all sensors on a site. For example, if two devices each send 15 alarms (below the GCXONE per-device threshold of 25), GCXONE allows them through individually — but Talos sees 30 total alarms for the site and blocks them.
- Error code: In Talos, this appears as the error code Alarm Limit Exceeded.

Key Capabilities

Configuration & Customization

The default thresholds are designed for general platform safety. For tenants with legitimate high-volume alarm requirements, these thresholds can be adjusted using Custom Properties:

- Configurable Thresholds: For specific high-priority tenants, the default 25-alarm limit can be increased (for example, to 50 or 100). This is set at the tenant or service provider level.
- Custom Property Name: The parameter used to adjust this is style.overflow.threshold.
- Isolation Duration: The defaultIsolationDuration (set at Service Provider level, in minutes) can be configured if a customer requires different notification suppression behavior.

Important Note for CSMs — Threshold changes must be coordinated with the R&D team and should only be applied after confirming that the high alarm volume is legitimate (e.g., industrial sites with high sensor activity) and not the result of a misconfigured device.

Best Practices

Key Reminder — Event Overflow is a protective feature — not a bug. When it activates, it means the system is working as designed to protect the platform. The priority is always to identify and correct the underlying device configuration that is generating excessive alarm volume.

- Switch from Basic Motion Detection to Smart Events (IVS) — Line Crossing and Intrusion Detection target real events only, eliminating the root cause of most overflow incidents.
- Run the manufacturer's test client before escalating to the platform team — if it also floods, the issue is confirmed to be the device, not GCXONE.
- Coordinate with the R&D team before adjusting thresholds — only increase limits after confirming the high alarm volume is legitimate and not the result of a misconfigured device.
- Notify the customer when overflow is active — inform them that alarms are being discarded so they can decide whether to be notified immediately or prefer a timed suppression window.

Additional Details

Troubleshooting — Identifying the Cause

When a device is blocked due to overflow, it is almost never a platform error. The root cause is nearly always a configuration issue at the physical site level.

1. Step 1 — Open the GCXONE dashboard and look for sensors showing a Blocked status or event.overflow log entries.
2. Step 2 — Access the physical NVR or camera logs to verify if it is genuinely producing a flood of events.
3. Step 3 — Run the manufacturer's test client (e.g., Hikvision Test Client, Dahua Config Tool). If the test client also floods, the issue is the device — not the platform.

Recommended Solutions

Once the cause is identified, use the following remediation approaches:

Recommended: Switch to Smart Events (IVS) — The most common root cause of overflow is the use of Basic Motion Detection, which triggers on any pixel change — wind, rain, reflections, insects. We strongly recommend switching to Intelligent Video System (IVS) events:

- Line Crossing Detection — triggers only when an object crosses a defined line.
- Intrusion Detection — triggers only when an object enters a defined zone.
- Human/Vehicle Filters — applies edge-side AI to ignore non-human/non-vehicle movement before sending any signal.

Additional Mitigation Options

- Reduce motion detection sensitivity: Lower the sensitivity setting on the camera or NVR, or increase the minimum object size threshold, so minor environmental changes do not trigger alarms.
- Adjust Threshold Time: Configure the device to require a sustained detection duration (e.g., 2 seconds of continuous motion) before sending an alarm — this filters out fleeting, non-threat triggers.
- Notify the customer: If a device enters overflow during an active monitoring period, inform the customer that alarms are being discarded. They should decide whether to be notified immediately when overflow starts, or prefer a timed suppression window.