

Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden“) werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen“ und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

Ereignisüberlauf

Updated 2 September 2026

Was Ereignisüberlauf bewirkt

Ereignisüberlauf ist ein plattformweiter Stabilitätsschutz in GCXONE, der das System automatisch vor Überflutung durch ein fehlerhaftes oder falsch konfiguriertes Gerät schützt. Ohne diesen Schutz könnte ein einzelner störender Sensor tausende Alarme in Minuten senden und möglicherweise die gesamte Alarmverarbeitungsinfrastruktur überlasten und alle Kunden auf der Plattform beeinträchtigen.

Warum es wichtig ist

Ohne Ereignisüberlauf-Schutz könnte ein einzelner störender Sensor die gesamte Plattform überfluten – nicht nur einen Kunden beeinträchtigen, sondern jeden Kunden, der die Infrastruktur teilt. Das Schwellwert-System stellt sicher, dass ein falsch konfiguriertes Gerät die Alarmverarbeitung für alle anderen nicht zum Erliegen bringen kann.

Wie es funktioniert

GCXONE – Geräteebene

GCXONE arbeitet mit einem plattformweiten Standard, um Ressourcenerschöpfung zu verhindern. Das System überwacht eingehende Alarme auf Ebene des einzelnen Geräts/Sensors:

- **Schwellwert:** Wenn ein einzelnes Gerät mehr als 25 Alarme innerhalb eines beliebigen 5-Minuten-Fensters sendet, wird der Überlauf-Schwellwert überschritten.
- **Alarmtyp:** Das System generiert einen internen Alarmtyp namens `event.overflow`, um den Zwischenfall zu protokollieren und signalisieren.

- Unterdrückung: Alle weiteren Alarme von diesem spezifischen Sensor werden für den Rest des 5-Minuten-Fensters verworfen.
- Wiederholung: Das System prüft neu am Anfang eines jeden neuen 5-Minuten-Fensters. Wenn die Alarmrate über dem Schwellwert bleibt, wird ein weiteres `event.overflow` ausgelöst und die Unterdrückung wird fortgesetzt.

Talos (CMS) – Standortebene

Selbst wenn einzelne Gerätealarmzählungen durch GCXONE durchkommen, können sie immer noch auf der CMS-Ebene (Evalink Talos) blockiert werden, die Überlauf-Logik auf Standortebene anwendet – über alle Geräte an einem Standort:

- Standort-Schwellwert: Talos aggregiert Alarme über alle Sensoren an einem Standort. Wenn zwei Geräte beispielsweise jeweils 15 Alarme senden (unter dem GCXONE Pro-Gerät-Schwellwert von 25), lässt GCXONE sie einzeln durch – aber Talos sieht 30 Gesamt-Alarme für den Standort und blockiert sie.
- Fehlercode: In Talos wird dies als Fehlercode `Alarm Limit Exceeded` angezeigt.

Wichtigste Fähigkeiten

Konfiguration und Anpassung

Die Standard-Schwellwerte sind für die allgemeine Plattformsicherheit ausgelegt. Für Mandanten mit legitimen High-Volume-Alarmanforderungen können diese Schwellwerte mit benutzerdefinierten Eigenschaften angepasst werden:

- Konfigurierbare Schwellwerte: Für spezifische Mandanten mit hoher Priorität kann die Standard-Alarmgrenze von 25 erhöht werden (z. B. auf 50 oder 100). Dies wird auf Mandanten- oder Dienstanbieter-Ebene festgelegt.
- Benutzerdefinierter Eigenschaftsname: Der Parameter zur Anpassung ist `style.overflow.threshold`.

- Isolationsdauer: Die defaultIsolationDuration (auf Dienstanbieter-Ebene festgelegt, in Minuten) kann konfiguriert werden, wenn ein Kunde ein unterschiedliches Benachrichtigungsunterdrückungsverhalten benötigt.

Wichtiger Hinweis für CSMS – Schwellwertänderungen müssen mit dem R&D-Team abgestimmt werden und sollten nur nach Bestätigung angewendet werden, dass das hohe Alarmvolumen legitim ist (z. B. Industriestandorte mit hoher Sensoraktivität) und nicht das Ergebnis einer fehlerhaft konfigurierten Gerät.

Best Practices

Wichtige Erinnerung – Ereignisüberlauf ist ein Schutzfeature – nicht ein Fehler. Wenn es aktiviert wird, bedeutet dies, dass das System wie konzipiert arbeitet, um die Plattform zu schützen. Die Priorität besteht immer darin, die zugrunde liegende Gerätekonfiguration zu identifizieren und zu korrigieren, die übermäßiges Alarmvolumen generiert.

- Wechsel von Basic Motion Detection zu Smart Events (IVS) – Line Crossing und Intrusion Detection zielen nur auf echte Ereignisse ab und eliminieren die Grundursache der meisten Überlauf-Zwischenfälle.
- Führen Sie den Test-Client des Herstellers aus, bevor Sie an das Plattform-Team eskalieren – wenn dieser auch Überlauf verursacht, ist das Problem bestätigt das Gerät, nicht GCXONE.
- Koordinieren Sie mit dem R&D-Team, bevor Sie Schwellwerte anpassen – erhöhen Sie Grenzwerte nur nach Bestätigung, dass das hohe Alarmvolumen legitim ist und nicht das Ergebnis einer fehlerhaft konfigurierten Gerät.
- Benachrichtigen Sie den Kunden, wenn Überlauf aktiv ist – informieren Sie ihn, dass Alarme verworfen werden, damit er entscheiden kann, ob er sofort benachrichtigt werden möchte oder ein zeitgestütztes Unterdrückungsfenster bevorzugt.

Zusätzliche Details

Fehlerbehebung – Ursachenidentifikation

Wenn ein Gerät aufgrund von Überlauf blockiert ist, ist dies fast nie ein Plattformfehler. Die Grundursache ist fast immer ein Konfigurationsproblem auf der physischen Standortebene.

1. Schritt 1 – Öffnen Sie das GCXONE-Dashboard und suchen Sie nach Sensoren mit Status Blockiert oder event.overflow-Protokolleinträgen.
2. Schritt 2 – Greifen Sie auf die physischen NVR- oder Kamera-Protokolle zu, um zu überprüfen, ob sie wirklich ein Flut von Ereignissen produziert.
3. Schritt 3 – Führen Sie den Test-Client des Herstellers aus (z. B. Hikvision Test Client, Dahua Config Tool). Wenn der Test-Client auch Überlauf verursacht, liegt das Problem beim Gerät – nicht bei der Plattform.

Empfohlene Lösungen

Nachdem die Ursache identifiziert wurde, verwenden Sie die folgenden Sanierungsansätze:

Empfohlen: Wechsel zu Smart Events (IVS) – Die häufigste Grundursache für Überlauf ist die Verwendung von Basic Motion Detection, die bei jeder Pixeländerung ausgelöst wird – Wind, Regen, Reflexionen, Insekten. Wir empfehlen dringend den Wechsel zu Intelligent Video System (IVS)-Ereignissen:

- Line Crossing Detection – wird ausgelöst, wenn ein Objekt eine definierte Linie überquert.
- Intrusion Detection – wird ausgelöst, wenn ein Objekt eine definierte Zone betritt.
- Human/Vehicle Filters – wendet edge-seitige KI an, um Nicht-Menschen/Nicht-Fahrzeug-Bewegungen zu ignorieren, bevor Signale gesendet werden.

Zusätzliche Lösungsansätze

- Reduzieren Sie die Empfindlichkeit der Bewegungserkennung: Senken Sie die Empfindlichkeitseinstellung auf der Kamera oder dem NVR, oder erhöhen Sie den Mindestgröße-Schwellwert für Objekte, damit kleine Umweltveränderungen keinen Alarm auslösen.

- Passen Sie die Schwellwert-Zeit an: Konfigurieren Sie das Gerät so, dass es eine anhaltende Erkennungsdauer erfordert (z. B. 2 Sekunden kontinuierliche Bewegung), bevor es einen Alarm sendet – dies filtert vorübergehende, nicht-bedrohliche Auslöser.
- Benachrichtigen Sie den Kunden: Wenn ein Gerät während einer aktiven Überwachungsperiode in Überlauf geht, informieren Sie den Kunden, dass Alarme verworfen werden. Sie sollten entscheiden, ob er sofort benachrichtigt werden soll, wenn der Überlauf beginnt, oder ein zeitgestütztes Unterdrückungsfenster bevorzugen.