

Disclaimer

Juridische disclaimer

Deze gids en de inhoud ervan (de "Gids") worden aangeboden door NXGEN. Alle rechten op de Gids en op de daarin vervatte intellectuele eigendom — met inbegrip van, maar niet beperkt tot, merken, handelsnamen, logo's en vergelijkbare tekens in of op de Gids — worden beschermd door de wet. Alle rechten, aanspraken en belangen met betrekking tot de Gids en de bijbehorende intellectuele-eigendomsrechten berusten en blijven bij NXGEN en zijn licentiegevers.

De Gids wordt kosteloos, "zoals deze is" en uitsluitend ter informatie verstrekt, zonder enige garantie. De Gids is niet bedoeld en evenmin geschikt om enige rechtsverhouding tot stand te brengen tussen de lezer en NXGEN of zijn gelieerde ondernemingen, met inbegrip van, maar niet beperkt tot, enige verplichting van NXGEN of zijn gelieerde ondernemingen jegens de lezer.

De verplichtingen van NXGEN en zijn gelieerde ondernemingen met betrekking tot door een klant afgenomen NXGEN-producten of -diensten worden uitsluitend beheerst door de voorwaarden van de overeenkomst waaronder die producten of diensten zijn afgenomen.

Ter verduidelijking

De lezer draagt het volledige risico ten aanzien van het gebruik, de resultaten en de prestaties van de Gids. Voor zover toegestaan door het toepasselijke recht wijst NXGEN alle garanties af, hetzij wettelijk, uitdrukkelijk of stilzwijgend — met inbegrip van, maar niet beperkt tot, stilzwijgende garanties van verhandelbaarheid, geschiktheid voor een bepaald doel, eigendom en niet-inbreuk op rechten van derden — evenals iedere aansprakelijkheid of garantie die voortvloeit uit suggesties, specificaties of voorbeelden met betrekking tot de Gids.

Overloop van evenementen

Updated 16 August 2026

Wat Event Overflow doet

Event Overflow is een platformbrede stabiliteitsbeveiliging in GCXONE die het systeem automatisch beschermt tegen een overbelasting door een defect of verkeerd geconfigureerd apparaat. Zonder deze beveiliging zou één enkele storende sensor binnen enkele minuten duizenden alarmen kunnen versturen, waardoor de volledige infrastructuur voor alarmverwerking mogelijk overbelast zou raken en alle klanten op het platform hier last van zouden krijgen.

Waarom dit belangrijk is

Zonder bescherming tegen overbelasting door gebeurtenissen zou één enkele storende sensor het hele platform kunnen overspoelen — met gevolgen niet alleen voor één klant, maar voor alle klanten die gebruikmaken van dezelfde infrastructuur. Het drempelsysteem zorgt ervoor dat één verkeerd geconfigureerd apparaat de alarmverwerking voor alle anderen niet kan lamleggen.

Hoe het werkt

GCXONE — Apparaatniveau

GCXONE hanteert een platformbrede standaardinstelling om te voorkomen dat bronnen uitgeput raken. Het systeem houdt toezicht op binnenkomende alarmen op het niveau van individuele apparaten/sensoren:

- Drempelwaarde: Als één apparaat binnen een willekeurig tijdsbestek van 5 minuten meer dan 25 alarmen verstuurt, wordt de overlooptrempel overschreden.

- Alarmtype: Het systeem genereert een intern alarmtype met de naam `event.overflow` om het incident te registreren en te signaleren.
- Onderdrukking: Alle verdere alarmen van die specifieke sensor worden voor de rest van het venster van 5 minuten genegeerd.
- Herhaling: Het systeem voert aan het begin van elk nieuw venster van 5 minuten een nieuwe controle uit. Als de alarmfrequentie boven de drempelwaarde blijft, wordt er opnieuw een `event.overflow` gegenereerd en wordt de onderdrukking voortgezet.

Talos (CMS) — op websiteniveau

Zelfs als het aantal alarmen van afzonderlijke apparaten via GCXONE wordt doorgegeven, kunnen deze nog steeds worden geblokkeerd op CMS-niveau (Evalink Talos), waar op locatieniveau een overlooplogica wordt toegepast — voor alle apparaten op een locatie:

- Drempelwaarde op locatieniveau: Talos telt de alarmen van alle sensoren op een locatie bij elkaar op. Als bijvoorbeeld twee apparaten elk 15 alarmen versturen (wat onder de GCXONE-drempelwaarde van 25 per apparaat ligt), laat GCXONE deze afzonderlijk door — maar Talos registreert in totaal 30 alarmen voor de locatie en blokkeert ze.
- Foutcode: In Talos wordt dit weergegeven als de foutcode „Alarmgrens overschreden“.

Belangrijkste mogelijkheden

Configuratie en aanpassing

De standaarddrempels zijn bedoeld om de algemene veiligheid van het platform te waarborgen. Voor tenants die om legitieme redenen grote hoeveelheden alarmen nodig hebben, kunnen deze drempels worden aangepast via ‘Aangepaste eigenschappen’:

- Configureerbare drempelwaarden: Voor bepaalde tenants met hoge prioriteit kan de standaardlimiet van 25 alarmen worden verhoogd (bijvoorbeeld naar 50 of 100). Dit wordt ingesteld op tenant- of serviceproviderniveau.

- Aangepaste eigenschapsnaam: De parameter waarmee dit kan worden aangepast, is ``style.overflow.threshold``.
- Duur van de isolatie: De ``defaultIsolationDuration`` (ingesteld op het niveau van de serviceprovider, in minuten) kan worden aangepast als een klant een andere manier van het onderdrukken van meldingen wenst.

Belangrijke opmerking voor CSM's — Wijzigingen in de drempelwaarden moeten worden afgestemd met het R&D-team en mogen pas worden doorgevoerd nadat is vastgesteld dat het hoge aantal alarmen terecht is (bijvoorbeeld op industriële locaties met veel sensoractiviteit) en niet het gevolg is van een verkeerd geconfigureerd apparaat.

Beste praktijken

Belangrijke herinnering — Event Overflow is een beveiligingsfunctie — geen bug. Wanneer deze functie wordt geactiveerd, betekent dit dat het systeem werkt zoals bedoeld om het platform te beschermen. De prioriteit ligt altijd bij het opsporen en corrigeren van de onderliggende apparaatconfiguratie die een te hoog alarmvolume veroorzaakt.

- Schakel over van standaard bewegingsdetectie naar slimme gebeurtenissen (IVS) — Detectie van het overschrijden van lijnen en inbraakdetectie richten zich uitsluitend op daadwerkelijke gebeurtenissen, waardoor de hoofdoorzaak van de meeste overloopincidenten wordt weggenomen.
- Voer de testclient van de fabrikant uit voordat je het probleem doorgeeft aan het platformteam — als deze ook vastloopt, is het probleem duidelijk het apparaat zelf en niet GCXONE.
- Overleg met het R&D-team voordat u de drempelwaarden aanpast — verhoog de limieten pas nadat u hebt vastgesteld dat het hoge aantal alarmen terecht is en niet het gevolg is van een verkeerd geconfigureerd apparaat.

- Breng de klant op de hoogte wanneer de overloopfunctie actief is — laat hem weten dat alarmen worden onderdrukt, zodat hij kan beslissen of hij onmiddellijk op de hoogte wil worden gesteld of liever een tijdsvenster voor onderdrukking kiest.

Aanvullende informatie

Problemen oplossen — De oorzaak achterhalen

Wanneer een apparaat door een overflow wordt geblokkeerd, is dat vrijwel nooit een platformfout. De hoofdoorzaak ligt bijna altijd in een configuratieprobleem op het niveau van de fysieke locatie.

1. Stap 1 — Open het GCXONE-dashboard en zoek naar sensoren met de status ‘Geblokkeerd’ of logboekvermeldingen met de trefwoord ‘event.overflow’.
2. Stap 2 — Bekijk de logbestanden van de fysieke NVR of camera om te controleren of er daadwerkelijk sprake is van een stortvloed aan gebeurtenissen.
3. Stap 3 — Start de testclient van de fabrikant (bijv. Hikvision Test Client, Dahua Config Tool). Als de testclient ook overspoeld raakt, ligt het probleem bij het apparaat — niet bij het platform.

Aanbevolen oplossingen

Zodra de oorzaak is vastgesteld, kunt u de volgende oplossingen toepassen:

Aanbevolen: Stap over op Smart Events (IVS) — De meest voorkomende oorzaak van een overloop is het gebruik van ‘Basic Motion Detection’, dat bij elke pixelverandering wordt geactiveerd — wind, regen, reflecties, insecten. We raden ten zeerste aan om over te schakelen naar gebeurtenissen van het Intelligent Video System (IVS):

- Detectie van het overschrijden van een lijn — wordt alleen geactiveerd wanneer een object een bepaalde lijn overschrijdt.
- Inbraakdetectie — wordt alleen geactiveerd wanneer een object een bepaalde zone binnenkomt.

- Filters voor personen en voertuigen — maakt gebruik van edge-side AI om bewegingen van niet-mensen of niet-voertuigen te negeren voordat er een signaal wordt verzonden.

Aanvullende maatregelen ter beperking van de gevolgen

- Verlaag de gevoeligheid van de bewegingsdetectie: Verlaag de gevoeligheidsinstelling op de camera of de NVR, of verhoog de drempelwaarde voor de minimale objectgrootte, zodat kleine veranderingen in de omgeving geen alarm activeren.
- Drempeltijd aanpassen: Stel het apparaat zo in dat er een aanhoudende detectieduur (bijvoorbeeld 2 seconden ononderbroken beweging) vereist is voordat er een alarm wordt verzonden — hierdoor worden vluchtige, niet-bedreigende triggers buiten beschouwing gelaten.
- De klant op de hoogte brengen: Als een apparaat tijdens een actieve bewakingsperiode in de overloopmodus terechtkomt, moet de klant worden geïnformeerd dat alarmen worden onderdrukt. De klant moet zelf beslissen of hij onmiddellijk op de hoogte wil worden gebracht zodra de overloop begint, of dat hij de voorkeur geeft aan een tijdsgebonden onderdrukingsperiode.