

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.

AI Analytics Overview

Updated 16 August 2026

What AI Analytics Does

AI Analytics in GCXONE uses artificial intelligence to analyze video events and distinguish real threats from environmental noise.

It processes incoming events in real time, identifying objects and evaluating their behavior before determining whether an event should be treated as a real alarm or suppressed.

- Reduces false alarms by up to 99%.
- Processes every event in real time before it reaches an operator.
- Identifies objects and evaluates behavior automatically.
- Ensures operators only see meaningful and actionable events.

Why It Matters

In many surveillance environments, most alarms are not real threats.

They are triggered by environmental factors such as lighting changes, weather conditions, reflections, or irrelevant objects. Over time, this creates alarm fatigue, slows down response times, and increases the risk of missing critical incidents.

AI Analytics solves this by applying intelligent filtering and decision logic to every event.

Instead of reacting to noise, operators only see events that have been analyzed and validated, improving accuracy, efficiency, and overall operational performance.

How It Works

AI Analytics processes each video event in two stages.

Identification The system detects and identifies all objects in the scene such as people, vehicles, or animals.

Decision After identification, the system applies predefined logic to determine whether the event should be considered a real alarm or suppressed.

This decision is based on configurable parameters:

- **Priority List** — Objects that always trigger a real alarm
- **White List** — Objects that may trigger alarms based on behavior
- **Black List** — Objects that are always ignored
- **Reject Unknown** — Filters environmental triggers such as wind or reflections

Only validated alarms are passed to operators, while false alarms are automatically suppressed.

Key Capabilities

- **False Alarm Reduction** — Reduces false alarms by up to 99% using AI-based filtering
- **Object Classification** — Detects and classifies people, vehicles, animals, and other objects in real time
- **Rule-Based Decision Logic** — Configurable lists control exactly which objects trigger alarms
- **Behavioral Analysis** — Evaluates movement patterns and activity over time
- **Real-Time Processing** — Analyzes events as they occur with no manual triggers required

AI-Powered False Alarm Filtering

AI Analytics filters out non-relevant triggers before they reach the operator, including lighting changes and shadows, camera vibration or movement, reflections and glare, and environmental motion such as trees or rain.

Detection Capabilities

DETECTION TYPE	WHAT IT DOES
Human Detection	Identifies human figures
Vehicle Detection	Identifies cars
Object Detection	Identifies objects that may trigger alarms

Alarm Quad Views

AI Analytics provides multi-frame context for each alarm event so operators can understand what happened before, during, and after the trigger.

- Pre-Alarm (Pre) — A frame from shortly before the event occurred, used for context leading up to the alarm.
- Preview — A quick reference frame to help operators rapidly assess the scene without switching views.
- Alarm — The exact frame captured at the moment the event triggered.
- Post Alarm — A frame from shortly after the event, showing what happened immediately following the trigger.

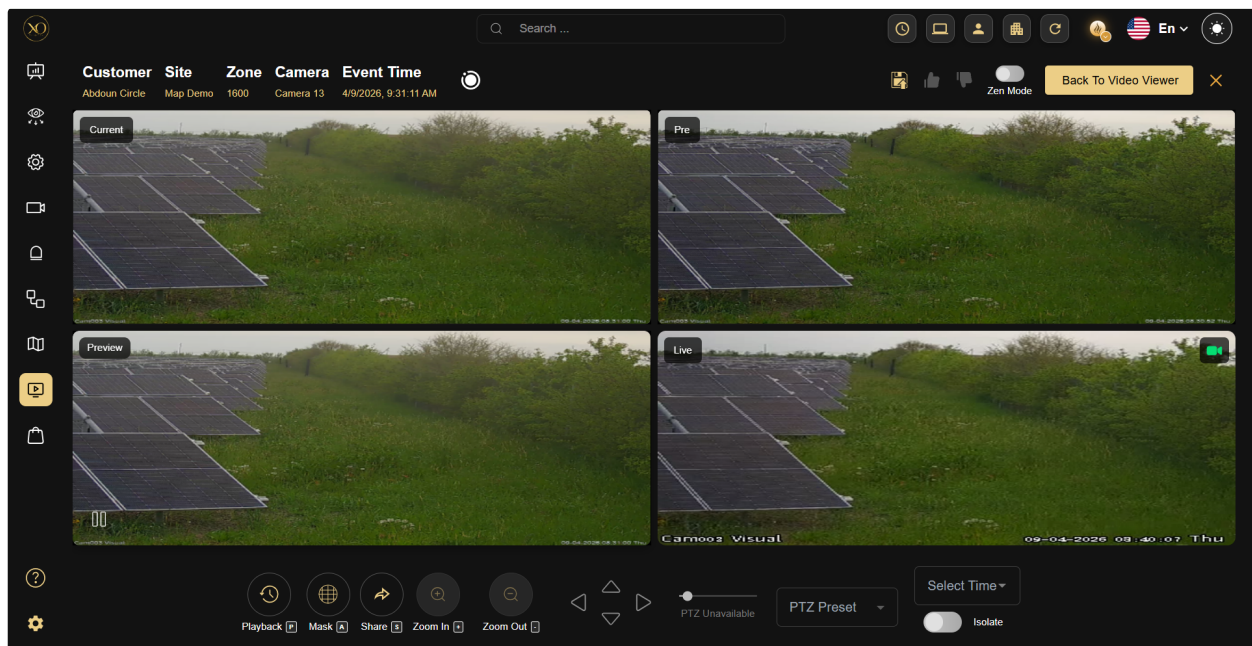


Figure 1: Alarm Quad View Interface — Displays Pre Alarm, Alarm, Post Alarm, and Preview frames together, enabling operators to quickly understand the full context of an event. Live, Playback, Jump Back, Mask, and Trigger Alarm are available as separate action buttons below the grid.

Fullscreen View — Double-click any Quad View tile — including pre-alarm, alarm, post-alarm, and preview — to expand it to full screen for clearer inspection. This allows operators to clearly verify events without struggling with small image sizes. Preview is now fully interactive and supports the same expansion behavior as the other tiles.

Alarm images in the Salvo Quad display in full without automatic zoom. Operators can review the complete camera frame directly in the quad view without opening a separate viewer. Zoom behavior is isolated per image and supports both optical and thermal camera feeds.

Supported Alarm Types

ALARM TYPE	DESCRIPTION
Motion Detection	Analyzes motion triggers for real vs. false
Intrusion Detection	Verifies human or vehicle presence in restricted areas
Line Crossing	Confirms object type crossing defined lines

Loitering Detection	Identifies person vs. other objects loitering
Tamper Detection	Distinguishes real tampering from environmental changes

Real-World Use Cases

- Environmental triggers such as shadows or weather changes are filtered out before they ever reach an operator.
- Instead of generic motion alerts, the system detects meaningful events such as intrusion or line crossing.
- Alarms are automatically classified before being presented to operators, reducing manual review effort.
- Security teams handle fewer, higher-quality alarms, improving response time and decision-making.

Best Practices

- Use smart events such as intrusion or tripwire instead of basic motion detection.
- Configure devices to provide sufficient context for analysis such as multiple frames.
- Ensure accurate time synchronization across systems.
- Maintain good camera quality and positioning for optimal detection accuracy.
- Avoid excessive environmental noise in camera views where possible.

Additional Details

Integration Workflow

AI Analytics operates as part of the GCXONE ecosystem.

1. A device triggers an alarm.
2. The event is processed and analyzed using AI.
3. The system determines whether the alarm is real or false.

4. Valid alarms are passed to operators, while false alarms are suppressed.

Scope and Limitations

What AI Analytics does:

- Analyzes video events using AI before they reach operators
- Filters environmental noise and reduces false alarms
- Applies configurable logic for accurate classification

What AI Analytics does not do:

- Does not replace physical security measures
- Does not guarantee 100% false alarm elimination
- Depends on proper configuration and camera quality