

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.

Alarm Configuration

Updated 16 August 2026

What Alarm Configuration Does

Alarm Configuration in GCXONE controls how alarms are processed, filtered, transmitted to the CMS, and presented to operators. It governs the full journey of every alarm — from detection to resolution.

Why It Matters

Without proper alarm configuration, verified alarms may never reach the CMS, operators may receive alarms without video context, or false alarms may flood the monitoring station. Correct configuration ensures only verified, actionable alarms reach operators — with full video evidence attached.

How It Works

The Alarm Lifecycle

Every alarm in GCXONE follows a strictly structured, traceable 5-step lifecycle:

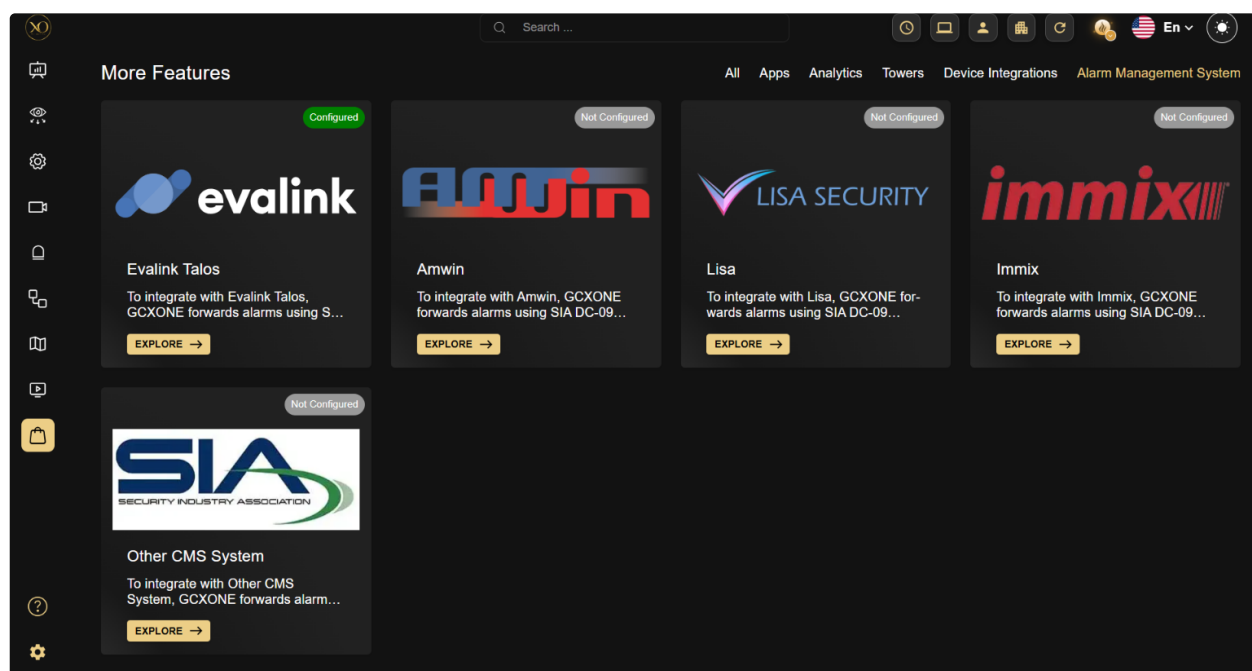
1. **Devices & Cameras** — Sensor detects an event and sends a signal to GCXONE.
2. **NOVA99x AI Filter** — AI pipeline evaluates the event. False alarms are discarded.
3. **Verified → CMS** — Confirmed alarms are forwarded via SIA DC-09 — the same protocol used for every CMS integration in GCXONE, including Evalink Talos.
4. **Operator Review** — CMS operator receives alarm with pre-event footage and live feed.
5. **Resolved + Audit** — Outcome is logged; immutable audit trail created.

How Alarms Reach Your CMS

GCXONE forwards every alarm to your CMS using the industry-standard SIA DC-09 protocol. You choose your CMS from a list of pre-integrated vendors — Evalink Talos, Amwin, Lisa, Immix — or select "Other CMS System" for a raw DC-09 channel to any unlisted receiver. All five options use the identical DC-09 configuration flow described below; only the vendor name differs.

Configuring DC-09 CMS Integration

Navigate to Marketplace → Alarm Management System.



1. Navigate to AMS in Marketplace — Go to Marketplace → Alarm Management System tab to filter available transmission integrations.
2. Select Your CMS Vendor — Click Explore on your CMS (Evalink Talos, Amwin, Lisa, or Immix). For unlisted vendors, select "Other CMS System" for a raw DC-09 channel.
3. Specify Connection Vectors — Enter the DC09 Receiver IP Address (WAN public IP) and DC09 Receiver Port (TCP port on the receiver firewall).
4. Initialize TCP Socket — GCXONE pings the receiver. A successful handshake updates the card to Configured. Alarms only flow for mapped sites.

5. SIA Details Display — Each device's Overview tab shows a SIA Details panel (Account Number, Encryption Key, Receiver IP, Receiver Port) for that device's DC-09 mapping.
6. Transmission Verification — Run a testing sequence via the diagnostics tab. Green lights confirm packets are acknowledged by the CMS.

Note

IMPORTANT — Most Common Failure: Account ID Mismatch: A mismatched Account ID is the most common cause of failed DC-09 transmissions. If the CMS expects "Site-A200" but GCXONE sends "Site_a200", the receiver silently discards the packet. Copy-paste from the CMS configuration rather than retyping.

Configuring Evalink Talos Integration

Evalink Talos uses the same SIA DC-09 flow as every other CMS vendor — there's no separate credential exchange. Open its card in Marketplace → Alarm Management System and click Configure to enter its Receiver IP and Port, exactly like Amwin, Lisa, or Immix.

Talos itself is a full monitoring-center platform with its own workflow engine (alarm routing, schedules, escalation) — see Talos Workflows for how alarms are handled once they arrive there.

AutoStream

AutoStream — a related feature that automatically opens live camera streams tied to Talos alarm zones.

See AutoStream – Zone-Based Camera Streaming for setup.

Key Capabilities

Alarm Flow Troubleshooting

SYMPTOM	CAUSE	FIX

Alarm shows Sent in GCXONE but CMS never receives it

Account ID mismatch

Copy-paste Account ID from CMS into the device's SIA Details; verify exact case and characters

AMS card shows red / disconnected

Firewall blocking DC09 IP or port

Verify WAN IP and TCP port are open

Real-World Use Cases

- A service provider connects GCXONE to an Immix CMS via DC-09 — operators receive alarms with pre-event footage embedded directly in the browser view.
- A new site goes live but alarms never arrive at the CMS — admin discovers an Account ID mismatch and corrects it by copy-pasting from the CMS.

Best Practices

- Always copy-paste the DC09 Account ID directly from the CMS — never retype it manually.
- Run the diagnostics transmission test after every configuration change before going live.