

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.

What is GCXONE

Updated 16 August 2026

Overview

GCXONE is a cloud-based platform for alarm management and security monitoring. It centralizes alarms, video surveillance, device health, workflows, and AI-based filtering into one interface, so operations don't depend on local, on-site infrastructure.

What Problems Does GCXONE Solve?

Many security operations centers and service providers face the same challenges:

- High volumes of false alarms caused by environmental factors such as movement, light, or weather
- Time-consuming manual verification processes
- Cameras going offline or degrading without being noticed
- Complex and slow onboarding of new customers, sites, and devices
- Limited visibility across distributed systems and locations

How Does GCXONE Work?

Every alarm follows a structured workflow:

- Devices, cameras, and sensors send events to GCXONE
- NOVA99x AI filters up to 99% of false alarms in real time
- Verified alarms are delivered to Talos with full context
- Operators review, confirm, or escalate incidents
- Automated workflows handle notifications, escalation, and SLA processes

- Every alarm is fully documented and stored in the audit log

Core Value

Up to 99% Reduction in False Alarms with NOVA99x

The built-in AI analyzes motion events in real time using:

- Object detection
- Dynamic motion analysis
- Tracking and re-identification

Faster Operations

- Zen Mode for rapid situational awareness
- Universal Search for instant access to data
- Role-based dashboards with clear KPIs

Health Check

Health Check continuously monitors all devices and detects issues early:

- Camera going offline or losing connectivity
- Black screen detection or obstruction
- Poor lighting conditions

Scalable Growth

- Bulk Import for rapid large-scale onboarding
- TowerGuard for centralized tower infrastructure monitoring
- Marketplace for instant activation of new features without redeployment

Genie – The Built-in AI Assistant

Genie is GCXONE's built-in AI assistant. It sits as a floating panel on the dashboard, always available. Users type their question and Genie pulls the relevant data or takes the action directly.

Genie handles five key areas:

- Alarms & System Insights: alarm summaries and system data analysis
- Ticket Management: open, close, or check ticket status by number
- VPN Requests: submit and manage VPN requests directly through the assistant
- Device Setup and Troubleshooting: step-by-step guidance for configuration and connectivity issues
- Adding Devices: start the device-creation flow directly from the chat

Platform Architecture

Multi-Tenant Structure

Clear hierarchy for maximum control:

- Service Provider, Customer, Site, Device, Sensor

Enables clean separation, clear ownership, and precise access control.

Multi-Level Operational Control

- Service Provider: global overview and SLA management
- Customer: customer-specific insights
- Site: local operations and incidents
- Device: detailed device-level monitoring

Role-Based Access

Each user only sees what is relevant to their role. Access is controlled through structured permissions and role configurations.

Integration with Talos

GCXONE and Talos work together:

- GCXONE filters and prioritizes alarms before they reach operators
- Only relevant events are forwarded
- Talos manages structured handling and escalation
- All actions are fully documented