

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.

Technical Specifications

Updated 23 September 2026

Covers: Onboarding & Adding Devices, NOVA99x False Alarm Filter, GC Edge, Local Agent. High-level engineering reference: how each part of GC Surge works, its limitations, and what will not work.

Implementation details (tech stack, tuning parameters) are out of scope.

Onboarding — Adding Devices

Overview

Onboarding connects a customer's cameras or alarm sources to GC Surge so their alarms flow into the Alarm Center. Every device belongs to a site; a site can hold many devices. Onboarding is reached from Configuration → Add sites & devices , which offers four entry points:

ENTRY POINT	WHAT IT DOES	BEST FOR
Guided setup (wizard)	Asks a few questions	detects the right connection method
Add sites manually	Opens the single-site form directly	Users who already know the connection method
Import from spreadsheet	Imports many sites and devices at once from a template	Larger rollouts
Universal device support	REST API / SMTP / FTP forwarding for one device	Devices that push their own alarms

A device is always attached to a site. Typing an existing site's name adds the camera to that site instead of creating a new one.

Connection methods

GC Surge supports four ways for a camera's alarms to reach the cloud. The guided wizard selects one automatically; the manual form auto-detects it from the reachability check and the device brand.

The deployment guides refer to the first three by number: Public is Mode 1, Private (local agent) is Mode 2, and GC Edge is Mode 3.

METHOD	HOW ALARMS REACH GC SURGE	USER REQUIREMENT
Public	GC Surge cloud reaches the camera directly (public IP)	DDNS
Private (local agent)	A local agent (desktop) on the site network bridges the camera to GC Surge and applies the configuration	Local agent installed on site; supported brand
GC Edge	A GC Edge unit on site connects to the camera's video stream and triggers the alarms	GC Edge installed and paired with the site key
Universal device support	The camera itself pushes alarms to an endpoint/address GC Surge provides; the user pastes the connection details into the camera	Camera can send alarms via API

Supported device brands

A device brand is supported when GC Surge can automatically inject the alarm configuration into the device — no manual device-side setup. The baseline supported brands are:

- Hikvision
- Dahua
- AXIS
- NX Witness

Hanwha and SpykeBox cameras run on the NX Witness platform — select NX Witness for them.

The live list in the platform is authoritative — it may include additional brands beyond this baseline. Always treat the platform's supported-brands dropdown as the current reference.

A camera not on the supported list is not blocked. It has two fallback paths:

- The camera can send its own alarms (API / FTP / SMTP). GC Surge generates the endpoint or address; the user pastes it into the camera's settings.

- The camera only streams video. A GC Edge unit on site watches the stream and produces the alarms.

Guided wizard — decision logic

The wizard collects the minimum it needs and routes to the right method across three steps:

1. Intent — new site, add a camera to an existing site, or bulk add.
2. Camera type — a brand from the list (auto-configured); my camera can send alarms (API/FTP/SMTP)
 - manual path; use GC Edge → edge path; I'm not sure → continue and detect.
3. Access (only when not already decided) — GC Surge can reach it directly → Public; private network only → Private (local agent); not sure → Private (safest default).

Single device — fields collected

FIELD	PUBLIC	PRIVATE	GC EDGE	NOTES
Site name	✓	✓	✓	Existing name = add to that site
Device IP or hostname	✓	✓	✓	Private IP for private/edge
Device brand	✓	✓	(GC Edge)	Supported-only dropdown; GC Edge toggle forces GC Edge
Web port + HTTPS toggle	✓	✓	✓	Public runs a port-reachability check
Video stream port	—	—	✓	GC Edge only
Username / password	✓	✓	✓	Camera credentials
On-site / contact info	Optional	Required if not on-site	Required if not on-site	Site key + instructions sent to on-site contact

Bulk import — what is and is not supported

The spreadsheet importer supports: multiple sites and devices in a single upload; all three connection types (public, private, edge); per-row validation before commit; a downloadable spreadsheet of failed rows; and a dedicated private device configuration step after import.

The Universal device support (REST API/SMTP/FTP) path is not supported in bulk import — that flow is per-device and interactive (the user copies connection details into each device individually).

NOVA99x — False Alarm Filter

NOVA99x is a noise-suppression module that filters up to 99% of false alarms, allowing security operations to scale without increasing headcount. It processes motion-triggered events in real time and classifies each event as a true alarm or a false alarm.

What it detects

NOVA99x uses the pre, current, and post images from each event (three frames) to detect motion and identify persons and vehicles — including personal cars, buses, trucks, and vans. It works with both optical and thermal sensors.

What it does NOT detect

- Animals
- Distant objects (small persons or vehicles far from the camera)
- Fast-moving cars
- Industrial vehicles and their parts

Camera compatibility

NOVA99x operates on event images rather than on specific camera streams — it is not tied to a particular set of camera models.

Limitations

- Cameras or alarm sources that send only a single image per event will have a very low true detection rate. NOVA99x is optimized for three-frame events.
- Video clips have lower throughput than three-frame events.
- Point cameras at the area of interest (entrance, clear field of vision). Avoid vegetation, support structures, or other obstructions that block the view.
- Detection accuracy decreases with distance and with lower illumination or contrast — night-vision cameras, thermal cameras, and low-light night scenes all reduce detection performance.

How it works (cloud)

NOVA99x processes the three event images in five steps:

1. Analyzes motion and identifies motion zones.
2. Analyzes image content and detects persons and vehicles.
3. Validates detection movement within the regions of interest and identifies stationary artifacts.
4. Filters out very fast and stationary objects, while keeping persons and moving vehicles.
5. Classifies the event based on the detections, the motion zones, and the configured parameters.

How it works on GC Edge (on-site)

On-site, NOVA99x analyzes the live feed and maintains a motion model. Once the motion model is triggered, the detection model activates to track objects and validate their movement.

GC Edge

GC Edge is the on-premise software appliance developed by NXGEN Technology AG that runs on a Windows PC at the customer site. It ingests video streams from IP cameras, runs AI motion detection

locally, and publishes alarm events to GC Surge. All video processing happens on-device — no video is sent to the cloud.

Minimum hardware requirements

COMPONENT	REQUIREMENT
Operating system	Windows 10 64-bit or Windows 11
CPU	4 physical cores minimum (1 camera); 8+ cores for 4–6 cameras
RAM	4 GB (1–2 cameras); 32 GB supports up to ~11–12 cameras
Storage	5 GB available minimum
Network	100 Mbps LAN to cameras (RTSP over TCP); outbound internet for alarm delivery
GPU	NVIDIA GPU with 4 GB+ VRAM for CUDA (optional — greatly improves performance)

How it works

Pairing — During initial setup, the operator enters the site key generated from the GC Surge portal into the GC Edge Manager application. GC Edge uses this key to authenticate with the platform, retrieve the list of devices registered to the site, and connect to each one automatically. No re-pairing is needed on restart.

Video ingestion — Each camera stream is handled independently. GC Edge connects directly to the camera over the local network, pulls the live video feed, and processes it entirely on the local machine. Hardware acceleration is used where available to minimize CPU usage.

AI detection — Video frames are analyzed locally by an AI model that detects and tracks people and vehicles in real time. On static scenes with no movement, AI analysis is suspended automatically and resumes the moment activity is detected.

Monitoring — The GC Edge Manager provides a live dashboard showing the status of every connected camera — whether it is active, the current detection state, and a live thumbnail view.

Connectivity — GC Edge requires a stable internet connection to deliver alarms to GC Surge and to allow the live feed to be fetched remotely.

Limitations

- A camera must be reachable on the local network; cameras on other networks or VLANs are out of reach.
- Detection quality depends on camera placement and scene conditions (same caveats as NOVA99x above).
- Capacity is bounded by the host PC — camera count scales with available CPU, memory, and GPU.
- A stable internet link is required for alarm delivery; while offline, alarms cannot be delivered to the platform.

Local Agent

The Local Agent is the Private (local agent) connection path. It configures cameras on a private network that cannot be reached directly from the cloud: the agent scans the site's local network and injects the alarm configuration into supported cameras it finds. Unsupported or unreachable cameras are skipped.

The Local Agent comes in two forms — a desktop agent (Windows) and a mobile app — that perform the same job.

Option A — Desktop Agent (Windows)

Use this when you are already connected to the same network as the cameras, or can remote into a machine that is. Install the Local Agent on any Windows PC on that network. Once running, the agent automatically detects which cameras belong to the site and configures them without further input. The

portal status updates to Configured once the agent finishes. No on-site visit is needed if you already have remote access to the client's network.

Option B — Mobile App

Use this when you do not have network access to the client site and need to send someone there in person.

When cameras are added for a site with no local agent, the system generates a site key and QR code.

Share this with the on-site person. They:

1. Install the Local Agent mobile app on their device.
2. Scan the QR code or enter the site key manually to link the app to the site.
3. Connect their device to the same local network as the cameras.
4. The app finds all cameras for the site and configures each reachable one automatically.
5. The portal status updates to Configured once complete.

The mobile app has no login — access is controlled through the site key. Only share the QR code with trusted personnel.

Supported device brands

- Hikvision
- Dahua
- AXIS
- NX Witness

Hanwha and SpykeBox cameras run on the NX Witness platform — select NX Witness for them.

Limitations

- The PC or mobile device must be on the same local network as the cameras during setup. Neither can reach cameras across different networks or VLANs.

- The mobile app has no login — access is controlled through the site key only. Share the QR code with trusted personnel only.
- If a camera is offline or unreachable at setup time, it will not be configured automatically. It can be retried once back online.
- Each site key is tied to a single site. If cameras span multiple sites, a separate site key is needed per site.