

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.

Analytics Dashboard Overview

Updated 8 October 2026

experience — not included in the PDF

Summary

Analytics is GC Surge's operational intelligence layer. It transforms raw alarm volume data into structured trend information that managers use to understand what is happening across their sites, identify problems before they become critical, and make evidence-based decisions about staffing, configuration, and operations. To open Analytics, click Analytics in the left sidebar. Covers: What Analytics Does, What Analytics Provides, Filters, KPI Cards, How to Read the Analytics Panels, Review Cadence, Best Practices.

What Analytics Does

Why It Matters

Without aggregated dashboards, security managers cannot identify which sites or cameras are generating disproportionate alarm volumes, track whether response quality is improving over time, or build the evidence base to justify staffing or technology decisions. Analytics provides the trend context that point-in-time dashboards cannot.

What Analytics Provides

Everything shown in Analytics is derived automatically from alarm events processed by the platform. No additional configuration is required to start seeing data.

- Alarm Flow Trend — the alarm trend over time as three series (Total, Filtered, Real), segmented by site and camera.

- Alarm density by hour — two panels (False and Real) showing when alarms peak during the day.
- Alarm Volume Overview — the filter rate, noisiest cameras, top sites, and peak alarm window at a glance.
- Operator Workload Intelligence — operator capacity and the value delivered by filtering, expressed as time saved, cost saved, and capacity and revenue potential for the current filters and period.
- Breakdown — per-site and per-device alarm counts (By site / Noisy devices tabs).

Each panel is explained in detail under [How to Read the Analytics Panels](#) below.

Filters

The Analytics screen includes three filter controls at the top of the page.

- Filter by Site — narrows all metrics and charts to a single site. Select All sites to view platform-wide data. There's no side-by-side compare view yet, so to compare two sites, load one and export or screenshot, then switch — or use the Breakdown panels (By site, Noisy devices), which already show per-site rows in one view. The underlying data is also available per site via API.
- Filter by Device — narrows all metrics and charts to a single camera within the selected site. Selecting a different camera replaces the current selection rather than adding to it. Select All devices to return to the site-wide view. The False Alarm Density by Hour and Real Alarm Density by Hour charts also support per-camera focus this way; for per-camera alarm-type breakdowns, use the Breakdown panel.
- Viewing Period — sets the time window: pick a preset range (up to Last month) or a custom From/To range. Shorter ranges suit daily operations; the weekly rollup is the standard for ROI and operator-performance reviews; longer ranges are best for trends and capacity planning; and a custom range for incident retrospectives. Very large windows take a few seconds to render.

When using filtered data for reporting, always note the filter state in your report. A screenshot showing platform-wide data presented as site-specific data is misleading.

KPI Cards

Seven KPI cards run across the top of the Analytics screen. All are scoped to the current Filter by Site, Filter by Device, and Viewing Period selections — switching from All sites to a single site re-scopes every card to that site only.

- **TOTAL ALARMS** — total alarm events received across all sites and devices in the selected period.
- **PASSED TO OPERATOR** — alarms that passed through NOVA99x and required human handling.
- **FILTERED BY NOVA99x** — alarms removed by AI before reaching any operator. The filter rate ($\text{Filtered} \div \text{Total} \times 100$) is shown in the Alarm Volume Overview panel below.
- **TIME SAVED** — cumulative operator hours saved through AI filtering in the period, calculated from average processing time $\times$ alarms filtered.
- **COST SAVED** — the monetary value of the time saved, based on your operator cost settings.
- **POTENTIAL CAPACITY INCREASE** — an estimate of the additional cameras your current team could handle at today's alarm rate and filter rate, without adding headcount.
- **POTENTIAL REVENUE INCREASE** — the estimated revenue potential from that additional camera capacity, based on your configured revenue-per-camera value.

How to Read the Analytics Panels

Filtered by NOVA99x (filter rate)

The percentage of ingested alarms NOVA99x filtered in the period — $\text{filtered alarms} \div \text{total ingested alarms} \times 100$. So 85% means 85 of every 100 ingested alarms were classified non-actionable and never reached an operator. This is a volume figure, not an accuracy figure: how often the AI was right comes from closure-tag feedback over time, not from this number. A very high rate isn't automatically good — if NOVA99x filters 99% of events on a perimeter camera that should report real intrusions, it may be over-filtering, so cross-check against the closure-tag distribution.

Alarm Flow Trend

A time-series of Total, Filtered and Real alarm counts. The three are plotted as independent lines rather than stacked: although $\text{Total} = \text{Filtered} + \text{Real}$, separate lines make it clear when the gap between Total and Real widens (more filtering) versus when they move in lockstep (no filtering effect). Use the Total / Filtered / Real toggles to hide series you don't need — the chart rescales automatically. Three patterns are worth knowing:

- Total spiking while Real stays flat — NOVA99x is doing its job; investigate the noise spike on the noisy-devices panel.
- Total flat but Real climbing — operations or filtering effectiveness changed; check for a new site going live or a NOVA99x reconfiguration.
- A diurnal pattern (peaks at dawn/dusk) — typically lighting-change false alarms, which the hour-density charts will confirm.

Alarm Volume Overview — Noisy devices and Peak window

Noisy devices is a count of cameras generating a disproportionately high false-alarm rate relative to the rest of your account. The Breakdown panel below names them by camera and site with each camera's share of all alarms, so you can prioritise masking and tuning.

Peak window is the recurring time-of-day when your team is under the most alarm pressure — useful for shift planning. If peak is consistently 17:00–18:00, that's where extra operator coverage or stricter NOVA99x thresholds pay off most. It shifts day to day, so read it over Last 7 days and Last 30 days to find the recurring pattern rather than reacting to a single day. For global deployments, peak by local time matters more than peak by UTC.

False Alarm Density by Hour

Shows how false alarms distribute across the hours of the day, which usually reveals their cause: dawn/dusk peaks point to lighting transitions (tune exposure or apply time-of-day masks); mid-afternoon peaks to tree shadows tracking the sun or HVAC steam venting on a cycle (mask the area or reschedule the cycle); late-night perimeter peaks to wildlife or vehicle lights from an adjacent road (targeted masking). It's most useful per camera, so combine it with the camera filter during tuning sessions.

Real Alarm Density by Hour

Shows when real alarms actually occur — the true threat window for your portfolio. Real alarms typically cluster outside business hours (nights, weekends) for commercial sites and during the day for residential. Compare the curve to your operator schedule: under-coverage at peak real-alarm hours means delayed events, weaker dispatch quality, and missed SLAs. Use it in scheduling reviews and to justify after-hours operator capacity.

Operator Workload Intelligence

Brings three workload measures together: average alarms handled per operator per hour versus your target throughput; the spread across operators (balanced, or is one operator carrying the team?); and projected capacity headroom. The headroom line — “could support X more cameras at current load” — divides free operator minutes by what one more camera would cost in operator time. It assumes today's

alarm rate per camera, NOVA99x filter rate and average processing time, so adding NOVA99x or retraining operators shifts it. Treat it as growth guidance, not a hiring contract.

Breakdown — By site vs Noisy devices

Two views of the same alarm data at different grains. By site rolls every alarm up by site — a quick “where is the volume coming from?” view, good for portfolio reporting and customer conversations. Noisy devices drills into individual cameras and ranks them by total alarm volume — the day-to-day tuning queue. Columns: Camera, Site, Total alarms, % of all alarms, and a Relative volume bar. The By site tab shows Site, Total alarms, Real alarms, Filter rate, and Alarm share. Both tabs rank rows #1, #2, #3. To act on a noisy camera, click into it to see its event timeline and Heatmap overlay (this usually identifies the physical source — a tree, a road, sun glare), open the camera in Configuration, draw a Mask over that source, and save. Watch the camera's row over the next 24–48 hours; the false-alarm count should drop noticeably. If masking doesn't help, camera angle or detection sensitivity is the next thing to tune.

Review Cadence

- Daily — Has alarm volume spiked significantly compared to the same time yesterday or last week? Are any previously quiet sites suddenly generating high volume?
- Weekly — Compare this week vs. last week. What changed? Did any operational events (new site activation, NOVA99x change, seasonal factors) correspond with volume changes?
- Monthly — strategic review. Is overall volume trending up because you are growing, or because alarm quality is degrading? Does staffing allocation match site activity patterns?

Best Practices

- Review Analytics weekly, not only during incidents. Trend problems are easier to fix when caught early.
- When a site shows a spike in alarm volume, cross-reference with Video Search to determine whether the increase represents real events or camera noise.

- Use the noisy camera list as an input to your NOVA99x configuration. Cameras generating high false-alarm volumes are the best candidates for AI filtering.
- Use Analytics for strategic review, not shift monitoring. The Alarm Center shows what is happening right now during a shift. Analytics is for weekly and monthly operational reviews — check it after connecting new sites to GC Surge, adding operators, or onboarding a large batch of cameras to measure the impact.
- Cross-reference the alarm density charts with your staffing schedule. If false alarm peaks and real alarm peaks overlap in the same hours, operators are processing noise during high-alert windows. Use this to adjust coverage or NOVA99x thresholds.

Empty State and Known Display Issue

When you first access Analytics on a new account, or view data for a site that was just activated, the screen shows zero or empty values. This is expected — data accumulates as cameras send events. After 24–48 hours of activity, meaningful data begins to appear.

The Noisy devices breakdown has its own empty state: it needs at least 24 hours of alarm volume and enough alarms per camera (typically 50 or more) for a false-alarm rate to be statistically meaningful, so brand-new accounts or those with very few cameras see a “no breakdown data” message. NOVA99x is always active — its classifications populate the breakdown as alarms arrive, rather than waiting for operator closure tags to accumulate.

A known display issue may show undefined labels in the Alarm Volume Overview panel when the page first loads. This is a transient display glitch. If the labels do not resolve after a few seconds, refresh the page.