

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.

Audit Logs

Updated 23 September 2026

Summary

The audit log is the immutable record of who did what, when, and to which object inside GC Surge. It exists for governance, support, and post-incident traceability. This page covers both tabs of the Audit & Compliance module: Audit Logs (platform action history) and Alarm Logs (alarm closure history). Covers: Audit Logs, Alarm Logs.

Audit Logs

What Gets Logged

The audit log captures every significant platform action, allowing reviewers to reconstruct events across the platform's core categories:

- **Accounts & Authentication:** User sign-ins, system access, and management of users, roles, or tenant profiles (Tenant Users).
- **Sites & Devices:** Site creation, single or multiple device registrations, configuration adjustments, and bulk device imports.
- **Device Import:** Bulk device import operations via Flash BulkImport — file uploads, import staging, processing, and completion events.
- **Analytics & Reports:** Event overview views, volume insights, alarm distributions, camera health checks, and email report configurations.
- **Billing & Subscriptions:** Subscription updates, invoice generations, payment method adjustments, and financial transaction history reviews.

Record Format

Each audit entry includes the following structured columns:

- **Date & Time:** The exact timestamp when the action occurred (rendered in UTC).
- **User:** The email address of the account or operator who performed the action.
- **Category:** The high-level module associated with the action (e.g., Billing, Device, Analytics, Site).
- **Sub Category:** The specific functional sub-grouping (e.g., Package, Events, Transactions, Payment Methods).
- **Action:** The explicit function executed by the user (e.g., Transaction History Viewed, Devices Listed, Analytics Events Overview Viewed).
- **Action Status:** The execution outcome, labeled in green as Success upon completion.
- **Source Entity:** The target database object or record affected (e.g., Invoice, PaymentMethod).
- **Log:** A human-readable text summary confirming the exact event context.

Video — available online at </api/media/file/Audit%20logs-1.mp4?prefix=media>

Searching and Filtering the Audit Log

The audit log UI supports precise dropdown-based filtering to streamline incident investigations and routine governance checks. Users can narrow down the paginated results using three main filter menus:

1. **Category:** Filter by major platform modules. Options include: Analytics, Authentication, Billing, Device Import, Devices, Reports, Sites, Subscription, Tenant, Users.

2. Sub Category: Context-dependent sub-filters that update based on your selected Category.

Sub-categories by category: Analytics (Alarm Distribution, Noisy Cameras, Overview, Volume Insights); Authentication (Email, Login, OTP); Billing (Payment Methods, Subscription, Transactions); Device Import (Import, Processing, Staging); Devices (Counters, Inventory, Management); Reports (Email Reports); Sites (Inventory, Site Access); Subscription (Pricing, Trial); Tenant (Onboarding, Service Provider); Users (Management, Registration).

3. Action: A fixed set of 15 action types that apply across all categories: Activate, Add, Complete, Edit, Export, Login, Register, Remove, Schedule, Select, Send, Start, Upload, Verify, View.

Immutability and Retention

- Write-Once Security: Audit records are strictly immutable. They cannot be edited, overwritten, or deleted by any user, including system administrators.
- 1-Year Retention: All audit compliance data is safely retained and accessible for a minimum of 12 months.

Alarm Logs

The Alarm Logs tab records the lifecycle of closed alarms. Every alarm that was acknowledged and resolved by an operator appears here, giving supervisors a searchable record of operator response times and closure quality across all sites.

Record Format

Each Alarm Log entry includes:

- Date & Time: When the alarm was originally triggered.
- Site: The site where the alarm originated.
- Device: The camera or sensor that detected the event.
- Closure tag: The tag the operator selected when closing the alarm.

- **Operator:** The operator who acknowledged and closed the alarm.
- **Acknowledged Status:** Closure status, shown as Closed.
- **Acknowledged At:** The timestamp when the alarm was acknowledged.
- **Assigned By:** The user who assigned the alarm to the operator.
- **Assigned At:** The timestamp when the alarm was assigned.
- **Time Taken:** Total elapsed time from acknowledgment to closure.
- **Actions:** An eye icon that opens the alarm detail view for that record.

Searching and Filtering Alarm Logs

Use the filter bar at the top of the Alarm Logs tab to narrow results:

1. **All sites:** Filter records to a specific site.
2. **All operators:** Filter by the operator who handled the alarm.
3. **All closure tags:** Narrow results to alarms closed with a specific closure tag.

Viewing Period (top right): defaults to Last 24 hours . Expand to select a longer range.

Viewing an Alarm

Clicking the eye icon in the **Actions** column opens the alarm detail view for that record. The modal displays the full context of the alarm event:

- **Breadcrumb:** Site name and Device name shown at the top left.
- **Date & Time:** The exact timestamp of the alarm.
- **Classification badge:** Shows REAL ALARM in green or the applicable classification.
- **(W) / (S) buttons:** Thumbs-up (W) and thumbs-down (S) rating controls for the alarm event.

- Video panels: Four clips shown simultaneously — Pre Alarm (footage before the event), Alarm (the trigger moment), Post Alarm (footage after the event), and a fourth panel showing additional camera footage.
- Closure metadata (top right corner): Acknowledged Status: Closed Acknowledged By: The operator who acknowledged the alarm. Acknowledged At: Timestamp of acknowledgment. Closure Tags: The tag applied at closure. Closure Notes: Any notes added by the operator at closure. Shows — if none were entered.