

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 Closure & Audit Trail

Updated 8 October 2026

experience — not included in the PDF

Summary

Alarm closure is the final action that records the handling outcome and releases the workload back to the site. Every closed alarm captures enough information for audit and performance analysis without forcing unnecessary typing. Covers: Alarm Closure, Audit Trail.

Alarm Closure

What You Enter at Closure

- Closure tag — a label that categorizes the outcome (GC Surge ships four by default: False Alarm, True Alarm, People Detected, Vehicle Detected). The standing list is curated by a Super Admin in the [Configure tags](#) dialog, reached from Alarm Center with Work Mode on Admin — see [Setup your alarm closure tags](#). Operators can also create one while closing an alarm: type a name that is not on the list in the Closure tags field and pick + Create “name”. The new tag joins the list everyone picks from, so agree naming with the team first.
- Optional description — free text for context the tag alone does not capture.
- Closure timestamp and operator identity are recorded automatically.

After Closure

The site view updates immediately once an alarm is closed. If the operator releases the site or ends their session, the site becomes available for another operator to take. All alarms remain in their closed state — no work is lost and no alarm is left open.

Managing Closure Tags

The available tag set is configured via the **Configure tags** dialog — in Alarm Center with **Work Mode** set to **Admin**, click **Tags** in the top-right area, next to **Help**. Closure tags then drive the **Operator feedback classification counts** chart in [Operator Performance](#), and the **Closure tag** column and filter on the **Alarm Logs** tab of [Audit Logs](#). Analytics reports on alarm volume and filtering rather than on tags. Consistent tags make performance analysis meaningful. Define your tag set before operators start processing alarms. Changing tags mid-deployment creates gaps in historical data.

If no closure tags have been configured, operators see a **Create closure tag** button in the **Close Alarms** modal. Clicking it opens the **Configure tags** dialog, where a tag can be added. An alarm cannot be closed until at least one tag exists.

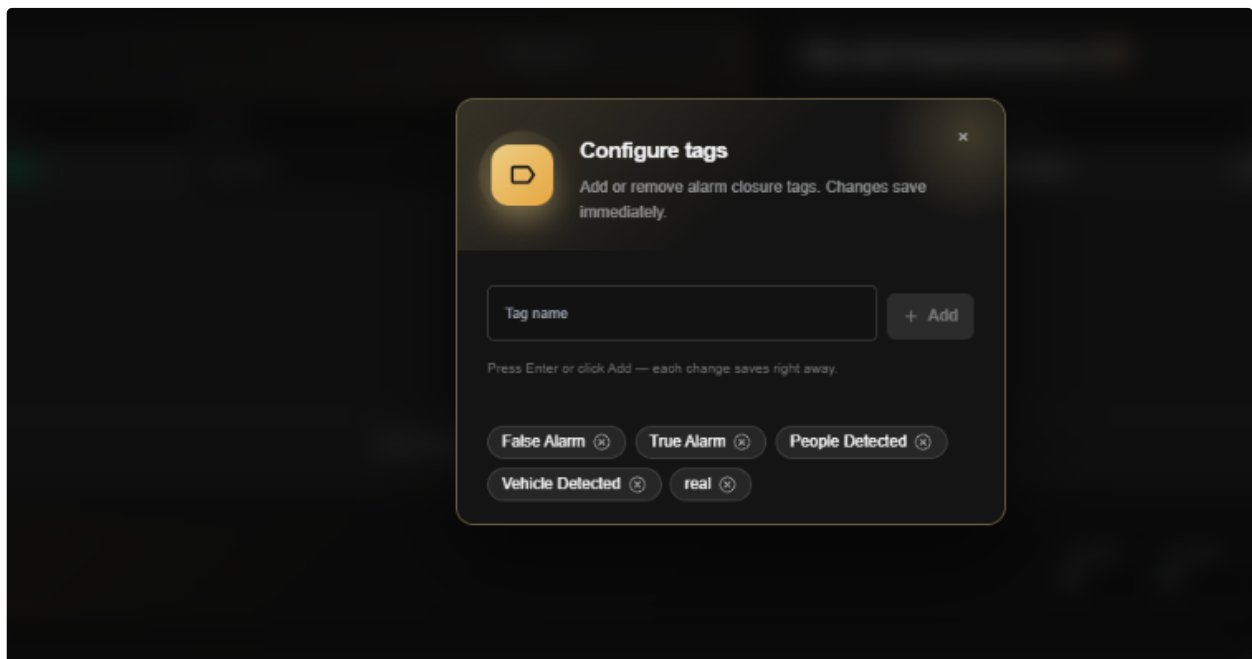


image-20260722-064124.png

Audit Trail

Every alarm has a traceable record that follows it from receipt through classification, operator handling, and closure. This trail supports customer trust, internal quality review, and any dispute about whether an alarm was received, shown, or handled on time.

The Full Chain

1. Alarm received from camera.
2. Normalized — site, camera, tenant, and timestamp attached.
3. Classified by NOVA99x as real or false.
4. Delivered into the operator monitoring workflow ([ZenMode](#)).
5. Taken by an operator — site ownership timestamp recorded.
6. Closed, escalated, or forwarded — tag, description, and closure timestamp recorded.

What the Trail Preserves

- Receipt time and camera source — regardless of downstream delays.
- Classification result and the basis for the decision.
- Operator identity and session context at every action.
- Closure outcome, tag, and any escalation or forwarding events.

Audit Log Guarantees

- Immutable — audit records cannot be edited or deleted by any user, including admins. Every entry is write-once.
- Minimum 1-year retention — audit data is retained for at least 12 months. See [Security and Data Retention Policy](#) for the full retention table.
- Searchable — filter the Audit Logs tab by Category , Sub Category , Action and User , and the Alarm Logs tab by Site , Operator and Closure tag ; both are scoped by the Viewing Period .



The full audit record is available in [Audit Logs](#).