



Emergency Alarm Deactivation, CCTV Checks, Tripwire Setup & Tailgating Management

Purpose: To provide standardised, auditable, and safe procedures for:

1. Temporarily deactivating the emergency alarm for authorized maintenance or testing;
2. Performing CCTV checks and exports (Dahua systems);
3. Setting up and testing camera tripwire/line-crossing alerts on Dahua equipment;
4. Managing incidents where members are detected tailgating access controls.

Safety first: Disabling or suppressing alarm systems creates real risk. Only authorized personnel may perform deactivation and only under controlled, documented circumstances with prior notification to UAC HQ and emergency services if required.

Scope:

Applies to all UAC Clubs using Dahua CCTV/NVR systems and onsite alarm systems. Covers Club Managers, Designated Safety Officers, authorised IT/security contractors, and Franchise Support.

Definitions

- Deactivation: Temporary silence or bypass of alarm/zone for maintenance or testing.
- Tripwire / Line-Crossing: Video analytic rule that triggers when an object crosses a drawn line.
- Tailgating: Unauthorized entry following an authorized person through an access point.

Authorization & Pre-Conditions

- Deactivation or tripwire changes must be authorised in writing by the Centre Manager + Franchise Support Officer (FSO).
- Notify UAC HQ and local emergency services if deactivation affects public-facing alarms.
- A minimum of two authorised staff must be present during deactivation/test.
- Ensure CCTV recording is active and backups are available before any change.
- Log the reason, scope, timing, personnel, and expected duration.

Emergency Alarm Deactivation (Controlled / Temporary)

When permitted

- Scheduled maintenance, alarm system testing, or equipment replacement.
- Emergency response training drills (with pre-notification).

Procedure

1. Request & Approve

- Submit Deactivation Request form to FSO at least 48 hours prior (or ASAP for emergency).
- Approval must include timeslot, zones affected, and contact details of responsible persons.

2. Pre-Work Checklist (before deactivation)

- Confirm approval & authorised personnel present (names & IDs).
- Notify UAC HQ, local emergency services (if required), and on-duty staff.
- Ensure CCTV & recording/storage are functioning; note storage capacity.
- Post signage at affected entrances: "Alarm Out of Service — Maintenance in Progress".

3. Deactivation

- Only authorised technician with access code performs deactivation at alarm panel.
- Record: date/time of deactivation, panel ID, zones disabled, technician name, and reason in the Alarm Deactivation Log.
- Keep the deactivation window as short as operationally required.

4. Monitoring During Deactivation

- Assign an on-site safety watcher (staff) to monitor affected areas physically and via CCTV.
- Maintain manual access control for vulnerable points (e.g., supervise garage doors).

5. Reactivation

- Technician re-enables system; perform a full system test (alarm, sensors, sirens).
- Log time of reactivation, test results, and tester name.
- Remove signage and notify HQ & emergency services that system is back online.

6. Post-Event

- Complete Incident/Deactivation Report and file in the compliance folder. Include CCTV extracts if any incident occurred during the window.
- Review cause and mitigation to avoid repeated deactivations.

Non-compliance

- Any unauthorized deactivation is a serious breach and must be escalated to Franchise Support and HQ immediately.

CCTV Review & Camera Check (Dahua Systems)

Access & Governance

- Only authorized users (Club Manager, Duty Manager, IT/FSO) use Dahua credentials.
- Use Dahua SmartPSS / DMSS / NVR Web UI per manufacturer guidance.
- Log each access in the CCTV Access Log (user, date/time, reason).

Daily/Weekly Camera Checks

- Daily: Confirm NVR is recording (green/normal status), check live view of critical cameras (entry, reception, gym floor, garage, basketball).
- Weekly: Playback 5–10 minutes of footage from each critical camera to verify clarity and timestamp accuracy.
- Monthly: Inspect camera lenses for dirt, alignment, and condensation; check night mode/IR function.

If Fault Found

- Record camera ID, observed issue, and time in the CCTV Maintenance Log.
- Reboot camera/NVR as first step; if unresolved, log and create a ticket to Dahua-certified technician.
- Export 48-hour footage pre-fault window for audit (if issue affects evidence).

Exporting Footage

- Use export function in SmartPSS/NVR; mark filename: Club_YYYYMMDD_CAM#_IncidentType.mp4.
- Save copy to secure USB and upload to HQ secure drive if required. Log export in CCTV Export Register (reason, exported by, chain of custody).

Setting Up Tripwire / Line-Crossing on Dahua (High-Level Steps)

Note: UI/version variations exist. Use vendor manual for exact UI navigation (SmartPSS or NVR Web).

Pre-check

- Ensure camera angle and resolution provide clear view of the intended detection zone.
- Confirm firmware is up to date and analytics features are supported by camera/NVR.

Configuration (authorized IT/tech)

1. Log in to Dahua SmartPSS or NVR web interface with admin credentials.
2. Open Camera Settings → Smart Detection (or Event → Smart depending on model).
3. Select Tripwire / Line Crossing:
 - Draw the line on the live preview where crossing is to be detected.
 - Set direction (both directions, inbound, or outbound).
 - Adjust sensitivity and object size filters (ignore very small/large objects to reduce false alarms).
4. Set Schedule: Define active hours for detection (e.g., after-hours only).
5. Linkage / Action:
 - Configure NVR to trigger alarm output, send email, push notification to SmartPSS/DMSS, or flag footage for easy retrieval.
 - Optionally trigger a snapshot or short clip export on event.
6. Save & Test:
 - Perform a live test (authorized person crosses the line) to confirm detection.
 - Adjust sensitivity and filters if too many false alarms or missed events.

Testing & Tuning

- Log each test result and final settings in the Tripwire Configuration Log.
- Re-test monthly or after physical changes to the environment.

Managing Tailgating Incidents (Detected by Tripwire / Access Control + CCTV)

Detection Pathways

- Tripwire in garage/entry + access control logs + CCTV playback = tailgating evidence.

Immediate Response (On Detection / After Hours Alarm)

1. If real-time alert (after hours):

- Duty staff to verify live feed.
- If unauthorized person is present, do not confront alone; call security or emergency services depending on risk.
- Record event and preserve footage.

2. If detected during hours:

- Retrieve footage and capture stills.
- Identify member (via access log) and possible follower.
- Approach calmly: staff to ask member to confirm who they let in and remind of tailgating policy.

Investigation & Logging

- Complete a Tailgating Incident Report with:
 - Date/time, camera IDs, access logs (card IDs), staff witness names, exported clip filename.
- Send report to Franchise Support Officer and HQ security team.

Member Management & Discipline

- If member intentionally let unauthorised person in, apply club policy (verbal warning → written warning → suspension depending on severity).
- For repeated or malicious incidents, revoke access privileges pending investigation.
- Maintain privacy: do not publish footage publicly—share only with authorised personnel and police if required.

Preventative Measures

- Enable door alarms on garage exits if possible.
- Use signage and member education: “No tailgating — swipe access only.”
- Consider access interlocks, turnstiles, or two-person verification in high-risk sites.
- Run periodic data matches between access logs and CCTV to find recurring patterns.

Logs & Records (Minimum Requirements)

- Alarm Deactivation Log (date/time, authorised by, zones, duration)
- CCTV Access Log (user, reason, start/end times)
- CCTV Export Register (file, reason, chain of custody)
- Tripwire Config Log (camera, line coordinates, sensitivity, test results)
- Tailgating Incident Report (videos attached)
- Incident/Investigation Report (outcome, disciplinary actions, corrective measures)

Keep records for minimum 12 months (or longer per local regulations / insurance requirements).

Privacy & Legal Compliance

- Only authorised persons may view or export footage.
- Inform members via signage that CCTV is in operation for safety.
- Comply with local privacy laws regarding surveillance and data access (store exports securely and delete per retention policy).
- Any release of footage to external parties (police, insurance) must be documented and authorized.

Training & Review

- Annual training for Club Managers and Duty Managers on alarm procedures, Dahua system use, tripwire setup basics, and tailgating response.
- After any major incident, conduct debrief and update SOP accordingly.
- Quarterly review of tripwire alerts and tailgating incidents by FSO.