

Falcon LogScale Migration Checklist

A practical acceptance guide for ingestion, parsers, detections, response, and security posture.

Sofia Wagner | Cybersecurity Engineer & Architect

Use this checklist when moving log sources and security workflows into Falcon LogScale or Falcon Next-Gen SIEM. Apply only the capabilities licensed and enabled for your destination. A check means there is evidence, an owner, and a recorded result; it does not mean a connector was merely created.

Migration record	Complete before the pilot
Scope / destination	_____
Migration owner / approver	_____
Pilot window / cutover window	_____
Evidence location / rollback owner	_____

1. Establish the migration baseline

- ☐ Inventory source feeds, current event rates, peak volume, retention requirements, and owners.
- ☐ Map critical searches, alerts, dashboards, reports, and response workflows to the new platform.
- ☐ Record which historical data must remain searchable and where. Do not assume live forwarding migrates old data.
- ☐ Agree on acceptable collection lag, loss tolerance, parser quality, and detection equivalence before testing.
- ☐ Confirm licensing, data-export rights, capacity, retention, and managed-service coverage.
- ☐ Define rollback triggers and preserve the current monitoring path until acceptance.

Gate 1: proceed when scope, success criteria, ownership, and rollback are approved. Keep environment-specific values in the internal working copy.

Prove delivery and parser quality

2. Connector readiness

- [] Choose push or pull deliberately; record the collection initiator and support owner.
- [] Confirm required event types, API permissions, source audit settings, and export entitlement.
- [] Match protocol, payload envelope, destination, parser, and routing. Syslog and HTTPS are not interchangeable.
- [] Test scoped credentials, encryption, certificate validation, expiration alerts, and rotation.
- [] Validate checkpoints, pagination, retries, throttling, and duplicate handling where applicable.
- [] Test outage recovery, queue limits, restart behavior, and alerts for silent sources.
- [] For ZIA, confirm NSS / Cloud NSS entitlement, supported feeds, forwarding compatibility, and event fidelity.

3. Parser readiness

- [] Retain representative raw samples, including failure, block, allow, administrative, and malformed events.
- [] Confirm event time, timezone, late-arrival behavior, and source-to-ingest lag.
- [] Normalize user, asset, network, action, and outcome fields needed by priority use cases.
- [] Preserve traceability to source records; record parser version and owner.
- [] Test identity and asset joins across at least two relevant sources.
- [] Replay samples after parser or source-format changes; document required-field coverage and error baselines.

Gate 2: expected datasets arrive within the agreed limits, parser tests pass, and gaps have an owner and documented impact. Evidence: sample events, counts, lag measurements, and recovery-test results.

Validate detections and security posture

4. Detection and workflow readiness

- ☐ Map built-in correlation templates to required sources and relevant ATT&CK behaviors.
- ☐ Confirm templates are enabled where intended; catalog availability alone is not active coverage.
- ☐ Test known-positive and known-benign activity, join keys, windows, thresholds, and exclusions.
- ☐ Confirm alerts include usable context and reach the intended analyst queue or case workflow.
- ☐ For third-party actions, validate the separate SOAR connector, scoped permissions, approval, audit, and recovery.
- ☐ Compare critical detection outcomes with the existing platform and record gaps or accepted differences.

5. Security posture and response readiness

- ☐ Reconcile protected assets against inventory; resolve missing, stale, or unhealthy sensors.
- ☐ Assign Active, Measured, or Cautious using privilege, exposure, business impact, fragility, and recovery readiness.
- ☐ Validate effective prevention settings and the current service-specific countermeasure approvals.
- ☐ Document approval boundaries for isolation, process termination, file removal, blocking, and restart.
- ☐ Check identity and cloud action prerequisites independently of endpoint posture.
- ☐ Test escalation contacts and a permitted response/recovery scenario; document separate DFIR responsibilities.
- ☐ Review SIEM access roles, strong authentication, audit visibility, retention, and export permissions.
- ☐ Give every posture exception and privileged integration credential an owner and review date.

Gate 3: priority detections work, response authority is clear, and security posture exceptions are explicitly accepted. Evidence: test alerts, approval records, role reviews, and recovery results.

Move monitoring without losing visibility

6. Parallel operation and cutover

- [] Run both platforms for an agreed observation window that includes representative peak and quiet periods.
- [] Compare event types, counts, freshness, required fields, and detection outcomes; account for different filtering or deduplication.
- [] Confirm dashboards, saved searches, case routing, notifications, and analyst access in the target platform.
- [] Confirm access to required historical records and preserve configuration, rule, and parser backups.
- [] Record final go/no-go approval and test the rollback procedure before redirecting production feeds.
- [] Validate freshness and alerts immediately after cutover; investigate unexpected volume changes.
- [] Decommission old forwarding only after acceptance, retention, and recovery obligations are satisfied; revoke unused credentials.

7. Operational handoff

- [] Assign owners for every source, credential, collector, parser, rule, posture exception, and recovery runbook.
- [] Enable alerts for source silence, ingestion lag, parser errors, queue pressure, credential expiry, and rule failures.
- [] Schedule early post-cutover reviews and recurring coverage, access, and posture reviews.
- [] Keep a known-gap register with business impact, compensating controls, owner, and target date.

Acceptance record	Result
Evidence / unresolved risks	_____
Security owner / business owner	_____
Go-live decision / date	_____
Rollback trigger / decision owner	_____

Companion: Falcon LogScale engineering article by Sofia Wagner. Official references:

- [Falcon Complete operating model](#)
- [LogScale ingest API](#)
- [Zscaler Internet Access integration](#)
- [CrowdStrike community content and dashboards](#)