



System	SAMPLE: Example Logistics Ltd., Distribution Centre 2
Site	Sample report, fictional organization
Auditor	Hans Study (sample data)
Date	10/5/2026, 12:46:53 AM

// Result

Overall score: 49%

Critical findings open

Pass 68 Fail 10 N/A 12 Unanswered 2 (of 92)

Flagged by severity: critical 1 high 5 medium 3 low 1

// Findings, critical and high first

1. [CRITICAL] Default credentials changed on all devices and accounts

Security and Access Control

Default credentials on a networked security device are an open door.

Field note: Sample note: not reviewed since the last upgrade. Re-check after the next maintenance window.

2. [HIGH] License type, expiry, and SMA status documented

Environment Overview

Lapsed SMA blocks upgrades and support exactly when you need them.

Field note: Sample note: configured but never tested. Test to be booked with the site operator.

3. [HIGH] SQL Server max server memory set explicitly

Servers and Roles

Left default, SQL takes everything and starves the OS and the roles sharing the box.

Field note: Sample note: differs between the primary and standby. Align and record the change.

4. [HIGH] Server network addresses and redirector configuration match the real topology and NAT

Network and Connectivity

A redirector address that doesn't match the real topology, a NAT boundary, or is left at localhost, breaks remote playback in a way that's maddening to diagnose.

Field note: Sample note: documented in a spreadsheet only, not in the system. Owner to be named.

5. [HIGH] Disk-threshold and archive-gap alerts configured

Health Monitoring and Alerts

Catch the drive filling and the gap forming before they cost you footage.

Field note: Sample note: not reviewed since the last upgrade. Re-check after the next maintenance window.



6. [HIGH] Federation vs distributed architecture deliberately chosen and documented

Integrations and Federation

The two models behave differently under WAN failure. Pick one on purpose, not by accident.

Field note: Sample note: differs between the primary and standby. Align and record the change.

7. [MEDIUM] 8.3 short-name creation disabled on archive volumes

Storage and Archives

Short-name generation adds write overhead on directories full of archive files.

Field note: Sample note: found on two of four servers. Fix scheduled for the next change window.

8. [MEDIUM] Audit logging enabled and retained

Security and Access Control

Without retained logs you can't answer who did what after an incident.

Field note: Sample note: configured but never tested. Test to be booked with the site operator.

9. [MEDIUM] GUS configured with defined maintenance windows

Backups, DR, and Upgrades

Genetec Update Service inside a controlled window, not whenever it feels like it.

Field note: Sample note: found on two of four servers. Fix scheduled for the next change window.

10. [LOW] Naming conventions documented and enforced

Roles, Processes, and Ownership

Enforced, not just written down once and ignored.

Field note: Sample note: documented in a spreadsheet only, not in the system. Owner to be named.

Want a second set of eyes on these findings? Genetec Health Check, hans.study/genetec-health-check/



// Full results, in section order

Environment Overview

[PASS] Current Security Center version and build recorded

[PASS] Patch level and last update date recorded

[FAIL] License type, expiry, and SMA status documented

[PASS] Camera, door, and active entity counts recorded

[NA] Servers and their assigned roles mapped

[PASS] Current network topology diagram exists

[PASS] StreamVault vs custom-build identified per server

[PASS] System owner and support contacts documented

[NA] As-built documentation exists and matches reality

[PASS] Security Center version is inside Genetec's supported lifecycle, and Windows and SQL versions are on the current support matrix

Servers and Roles

[PASS] All active roles mapped to servers (Directory, Archiver, Access Manager, Media Router, Health Monitor)

[PASS] Directory not co-located with Archiver above ~50 cameras

[PASS] Power plan set to High Performance on every server

[FAIL] SQL Server max server memory set explicitly

[PASS] SQL edition and per-database headroom checked against the Directory database size

[PASS] TempDB on a dedicated drive where possible

[PASS] CPU, memory, and disk baselined under production load

[NA] Archiver aggregate ingest kept under two-thirds of its rated ceiling

[PASS] Server hostnames follow a documented naming convention

[PASS] OS drive protected by RAID and separate from video archive

[PASS] Directory failover configured and tested

Storage and Archives

[PASS] Archive storage sized for peak bitrate with 20 to 30 percent headroom

[PASS] Archive volumes on RAID 6 or equivalent redundancy

[PASS] Windows Search indexing disabled on archive volumes

[FAIL] 8.3 short-name creation disabled on archive volumes

[NA] NTFS 64 KB allocation unit on video volumes

[PASS] Archive paths and secondary/failover paths documented

[PASS] Retention period matches policy and verified against real usage

[PASS] Actual retention per camera checked against configured retention, and protected video reviewed

[PASS] Archive transfer, redundant archiving, or failover archiving chosen deliberately for the sites that need it

[NA] Archive drive usage reviewed on a schedule

[PASS] AV exclusions applied for GenetecServer.exe, GenetecWatchdog.exe, and sqlservr.exe, archive paths, and .g64/.g64x files

Network and Connectivity

[PASS] Receive and transmit buffers raised to the driver maximum (4096 on most Intel NICs) on video-facing adapters

[PASS] Camera, client, and management traffic separated

[PASS] QoS marking applied to video and control traffic

[FAIL] Server network addresses and redirector configuration match the real topology and NAT

[PASS] Redirect addresses re-verified after last topology change or migration

[NOT CHECKED] Multicast configuration validated where used



[PASS] Aggregate client bandwidth checked against workstation links
[PASS] Firewall rules documented for Genetec ports
[PASS] NTP time sync consistent across servers, cameras, and controllers

Health Monitoring and Alerts

[PASS] Health Monitor role online, on an appropriate server, database healthy, health event retention set
[NA] System status used operationally, not just on demand
[NA] Health alarms routed to a person or a ticket queue
[PASS] Health history reviewed on a schedule
[PASS] Camera-offline and recording-failure alerts configured
[FAIL] Disk-threshold and archive-gap alerts configured
[PASS] Role/server-down alerts configured and tested
[PASS] Someone owns acting on alerts, not just receiving them

Security and Access Control

[PASS] RBAC configured on least privilege, no blanket admin
[PASS] Active Directory integration in place for auth and lifecycle
[FAIL] Default credentials changed on all devices and accounts
[PASS] TLS and certificates configured and not expired
[PASS] Directory certificate validation and TLS configured per the 5.14 hardening guide
[PASS] Communications encrypted per the Genetec hardening guide
[PASS] Genetec Security Center Hardening Guide baseline applied
[NA] CIS baseline applied to servers (StreamVault ships to a CIS Level 1 baseline with documented exceptions, tested)
[FAIL] Audit logging enabled and retained
[PASS] Service accounts documented with scoped permissions
[NA] Synergis cardholder data and access RBAC reviewed

Cameras and Field Devices

[PASS] Standard camera profiles defined and applied, not per-camera drift
[PASS] H.265 used where cameras and licences support it, and operator workstations have hardware H.265 decode
[PASS] Stream separation in place: high-quality record, low-quality live
[PASS] Recording mode set per area and policy, not uniform continuous
[PASS] Default device credentials changed
[PASS] Firmware versions recorded and on a managed baseline
[PASS] Device time sync confirmed
[PASS] Door controllers (HID, Mercury, Axis, and Synergis Cloud Link) inventoried with firmware recorded

Integrations and Federation

[FAIL] Federation vs distributed architecture deliberately chosen and documented
[NA] If separate Security Center systems share cardholders, Global Cardholder Synchronization is configured and sync is verified
[NOT CHECKED] WAN reliability validated for the chosen multi-site model
[PASS] Federation host (running the Security Center Federation or Omnicast Federation role) connectivity to federated systems verified
[PASS] Third-party integrations inventoried (intrusion, LPR, analytics, etc.)
[PASS] Integration accounts and API access documented and scoped
[PASS] Plugin and SDK versions recorded and supported

Backups, DR, and Upgrades



[PASS] Directory and every role database (Archiver, Access Manager, and others) backed up through Server Admin, copied off the host, restore tested

[NA] Backup restore tested, not just configured

[PASS] Configuration export retained off-box

[PASS] Rollback procedure documented for changes and upgrades

[FAIL] GUS configured with defined maintenance windows

[PASS] Upgrade path validated, not deploying .0 releases straight to production

[PASS] Windows updates tested before hitting Genetec servers

[NA] DR plan exists for Directory loss and site loss

[PASS] Update-combination compatibility checked before applying

Roles, Processes, and Ownership

[PASS] A single accountable owner for end-to-end system health

[PASS] RACI defined across network, server, storage, and Genetec app

[PASS] Change management process exists and is followed

[PASS] Maintenance schedule documented and assigned

[PASS] Integrator handoff and as-built documentation complete

[PASS] Escalation path defined for incidents

[FAIL] Naming conventions documented and enforced

[PASS] Review cadence scheduled (quarterly or annual)