SERVICE SPECIFICATION / PHYSICAL SECURITY

Security systems integration

GHT-SVC-022 • Revision 1.0 • 06 September 2026 • 1 / 3

Supported APIs and standards can correlate video, access, intrusion, intercom, visitor, and identity events.

Intended outcome

Tested event and identity connections with permission records, correlated logs, failure alerts, recovery tests, and an operator runbook.

Service scope

A security integration may correlate access events with video, issue temporary visitor credentials, trigger an intercom workflow, synchronize identities, or route alarms into a shared operating view. The supported API or standard, licensing, versions, data ownership, and permissions determine whether the design is sustainable.

Integration does not remove the need to commission each underlying system independently. Each automated action needs a defined trigger, authorization, audit record, retry or timeout behavior, and manual fallback.

How the system fits together

01 Systems of record	Identity, credentials, devices, schedules, visitors, incidents
02 Interface	Supported API, webhook, SDK, connector, ONVIF or SIA data model
03 Policy	Authorization, mapping, transformation, retry, deduplication, retention
04 Operations	Logs, health, alerts, manual fallback, upgrade and owner process

Typical project triggers

- Operators switch among systems to reconstruct one event
- Duplicate identity records create slow or inconsistent revocation
- An unsupported custom link breaks during upgrades
- Automated actions lack audit records, failure alerts, or a manual path

Delivery and acceptance

The final project scope identifies quantities, locations, dependencies, and the evidence required at each delivery stage.

01 Map the current workflow

Identify systems, identities, event sources, operator steps, permissions, versions, licensing, data retention, and failure pain points.

Acceptance evidence: Current-state sequence diagram, data-owner matrix, interface inventory, and version/licensing record.

02 Design the contract

Define source of truth, events, fields, actions, authorization, rate limits, retries, deduplication, logging, fallback, and change ownership.

Acceptance evidence: Future-state sequence, field and event map, permission model, failure table, and acceptance cases.

03 Configure in stages

Build in a controlled environment, protect credentials, constrain privileges, enable logs, and release workflows in observable increments.

Acceptance evidence: Configuration record, secret-ownership record without secret values, change log, test identities, and rollback plan.

04 Prove normal and failed paths

Test success, duplicates, delay, unavailable systems, revoked access, unauthorized actions, retries, recovery, audit lookup, and manual fallback.

Acceptance evidence: Acceptance-case results, correlated event samples, alert evidence, rollback result, and owner runbook.

Handover deliverables

- Current- and future-state sequence diagrams
- Interface, event, field, and permission mapping
- Failure-mode and rollback plan
- Normal, exception, security, and recovery acceptance results
- Version, ownership, monitoring, and change runbook

Closeout: GHT and the customer review the agreed evidence, record unresolved exceptions and owners, and confirm acceptance against the signed project scope.

Planning and scope boundaries

Customer and site inputs

- System owners, versions, licensing, supported interfaces, and update cadence
- Source-of-record identities, device records, event fields, and retention boundaries
- Trigger, action, approval, timing, retry, and duplicate behavior
- Service accounts, permissions, credential ownership, and audit requirements
- Failure notification, manual fallback, maintenance window, and rollback process

Constraints and coordination

- An integration is limited by documented vendor interfaces, licensing, versions, rate limits, and support policy
- Cross-system commands can amplify a bad identity, rule, or compromised account
- Biometric, video, visitor, and identity data can carry privacy and retention obligations
- Upgrades to either platform can require regression testing or connector changes

Commercial scope and responsibilities

This specification describes the service framework. The signed statement of work defines included equipment, quantities, software licenses, integrations, access windows, schedule, pricing, warranty, and support coverage. Additional construction, electrical work, recurring subscriptions, and ongoing support require an explicit line item.

The customer appoints an acceptance owner and provides authorized access, required site information, and decisions. GHT records assumptions, coordinates assigned work, and submits changes for agreement before expanding the scope.

Technical references

ONVIF — Profiles overview | Source review: 2026-08-20

Security Industry Association — At-a-Glance Guide to SIA Standards | Source review: 2026-08-20

National Institute of Standards and Technology — SP 800-207: Zero Trust Architecture | Source review: 2026-08-20

Service guide and project discussion | Source review: 2026-09-06