

DOC-2026-365 — SynthCloudConnect — DICOM Conformance Statement

Document number: DOC-2026-365 **Title:** SynthCloudConnect — DICOM Conformance Statement **Version:** v4
Category: DICOM Conformance Statement **Release version:** 1.0.2.110 **Product:** SynthCloudConnect 1.0.2.110 (Phase 1) **Classification:** Non-device software (FD&C Act §520(o)(1)(D)) **Owner:** Synthology Healthcare Solutions Group (SHSG) **Effective date:** (on approval) **Cross-references:** DCR-2026-046 v2 (Product Definition); DCR-2026-047 v2 (Regulatory Classification); DOC-2026-074 (Router DICOM Conformance — SCC's primary on-prem peer).

This statement is structured per DICOM PS3.2 (Conformance) 2024c. SCC is a **DICOMweb-only** product (PS3.18 Web Services); it does **not** speak classical DIMSE protocols (no C-STORE, C-FIND, C-MOVE, C-GET, C-ECHO). A DICOMweb origin still warrants an Implementation Class UID per PS3.5 Section 9 (UID Encoding Rules) for objects in transit.

1. Introduction

1.1 Revision History

Version	Date	Change
1	2026-05-16	Initial release (SCC v1.0.0.x Phase 1).

1.2 Audience

Engineers integrating AI inference vendors with hospital on-prem infrastructure via SynthCloudConnect's cloud-side relay. Assumes DICOMweb familiarity at the PS3.18 STOW-RS / WADO-RS / QIDO-RS level.

1.3 Remarks

SCC is a cross-site DICOM **result relay** in the cloud. It is a pure transit / store-and-forward intermediary — every DICOM instance that flows through SCC is **pseudonymized at the upstream source** (at the AI inference vendor before STOW, or at the on-prem ImageStream Router on the outbound leg). The re-identification keypair lives on the customer's on-prem side; SCC never holds it and cannot resolve pseudonyms back to clinical identifiers. SCC's operator surface therefore exposes operational aggregates (counters, queue depth, throughput, error rate) but no per-study clinical browsing surface — there's no clinically-actionable identifier inside SCC for a customer view to display.

SCC plays three roles in the DICOMweb information model:

1. **STOW-RS Origin Server** — accepts study POSTs from authenticated senders (AI inference vendors); persists Part 10 bytes verbatim into a per-tenant SQLCipher hold queue.

2. **WADO-RS Origin Server** — serves the same Part 10 bytes back to an authenticated puller (the customer's on-prem ImageStream Router) in `multipart/related; type="application/dicom"` form.
3. **QIDO-RS Origin Server** — exposes a study-level index over the hold queue so the Router can sweep for unfetched studies.

SCC is **not** a long-term archive (default TTL 72 hours; cold-storage handoff optional). It is **not** a DICOMweb Worklist (no UPS-RS), is **not** a Rendering Origin (no rendered-frame retrieval), and does **not** transcode pixel data.

1.4 Terms and Definitions

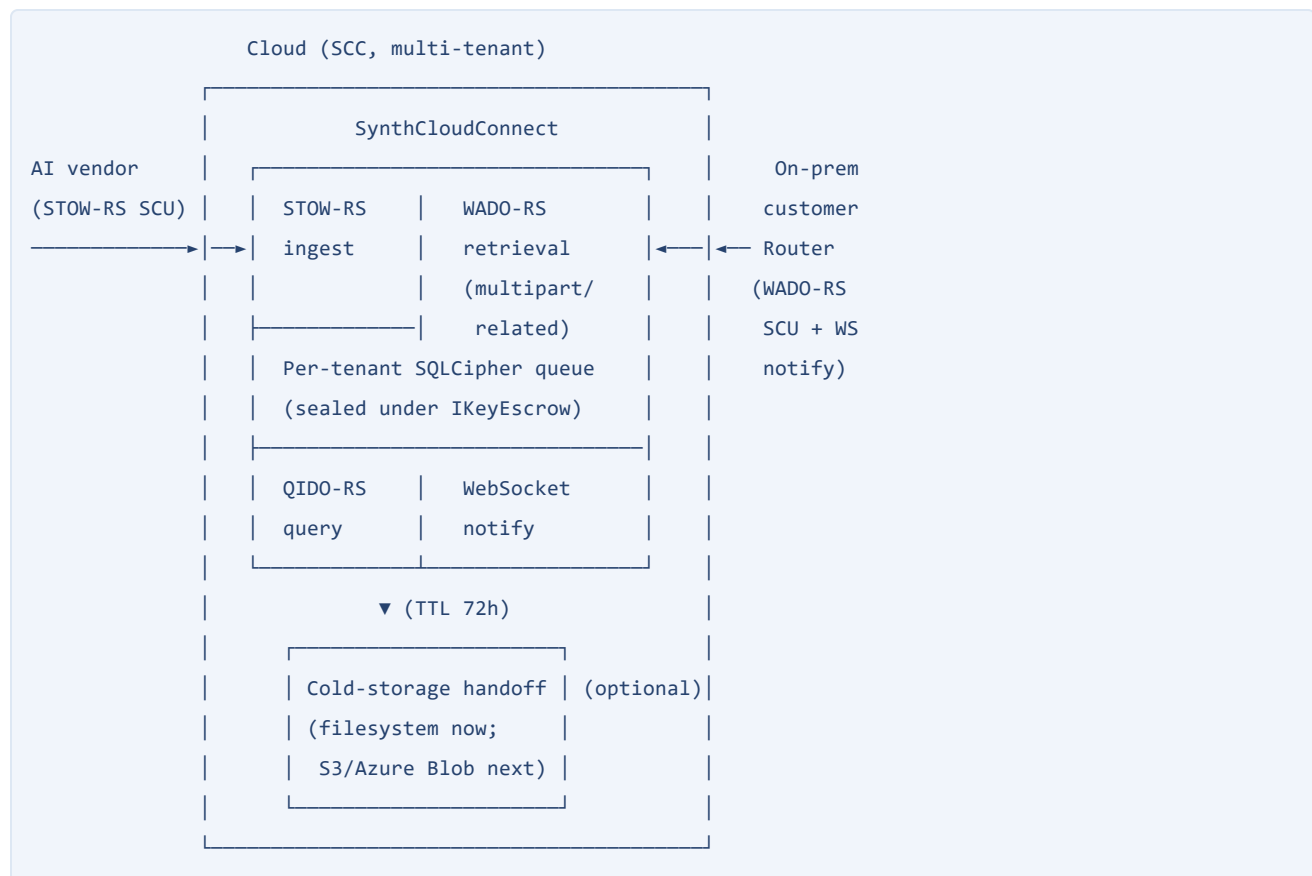
Per PS3.3 and PS3.18. SCC-specific terms: - **Tenant** — single customer's logical channel through SCC; each has its own SQLCipher hold queue at `queue/<tenant>.db`, sealed under IKeyEscrow scope `SynthCloudConnectHoldQueue_<tenant>`. - **Hold queue** — bounded-lifetime storage of in-transit studies awaiting Router pickup. Default retention 72h. - **Cold storage handoff** — optional archival to a configured directory before TTL purge (PS3.10 Part 10 files preserved with metadata).

1.5 Conformance References

- DICOM PS3.1–PS3.18, 2024c (especially PS3.18 Web Services)
- IHE RAD Cross-Enterprise Document Sharing for Imaging (XDS-I.b) — SCC's role analogous to "Imaging Document Source"
- HTTP/1.1 (RFC 7230–7235), TLS 1.2/1.3 (RFC 8446) — wire transport

2. Implementation Model

2.1 Application Data Flow



2.2 Functional Definitions

- **STOW-RS Origin Server** — receives `POST /dicomweb/{tenantId}/studies` with `multipart/related; type="application/dicom"` body; commits each Part 10 to the tenant's SQLCipher queue; emits a notification frame on the WebSocket relay so the Router can pull.
- **WADO-RS Origin Server** — serves `GET /dicomweb/{tenantId}/studies/{studyUid}` returning the full study as `multipart/related; type="application/dicom"`.
- **QIDO-RS Origin Server** — serves `GET /dicomweb/{tenantId}/studies?...` returning the in-queue study index as `application/dicom+json`.
- **DELETE channel** — `DELETE /dicomweb/{tenantId}/studies/{studyUid}` is the Router's acknowledgement that the study has been delivered on-prem; SCC drops it from the queue.

2.3 Sequencing of Real-World Activities

1. Vendor authenticates to SCC (Cloudflare Access JWT or mTLS at the tenant endpoint; auth scheme is per-tenant configurable).
2. Vendor `POST /dicomweb/{tenantId}/studies` with multipart Part 10 payload. SCC validates content type, parses each part as a DICOM instance via fo-dicom 5.x, writes to the tenant's SQLCipher DB, returns `200`

OK with a STOW-RS response document.

3. SCC's `WebSocketNotificationBroker` emits a `study_available` frame to any Router WebSocket connection for that tenant.
4. Router opens an HTTPS WADO-RS retrieval; SCC streams the multipart body.
5. Router locally distributes per its rules engine, then issues `DELETE /dicomweb/{tenantId}/studies/{studyUid}` to acknowledge.
6. If the Router is offline, the study sits in the hold queue. On reconnect the Router can either receive a fresh notification (for studies still within TTL but not yet acked) or sweep the queue via QIDO-RS.
7. If TTL expires without ack, `HoldQueueSweepService` archives to `ColdStorageDir` (when configured) and purges the queue row.

3. AE / Origin-Server Specifications

3.1 STOW-RS Origin Server

3.1.1 SOP Classes Supported

SCC accepts **all Storage SOP Classes** (PS3.4 Annex B.4). The origin server does not enforce an Abstract Syntax whitelist — any DICOM instance whose transfer syntax matches §3.1.2 is committed verbatim.

3.1.2 Transfer Syntaxes

Any transfer syntax registered in PS3.5 may be passed through SCC without transcoding. SCC does NOT decode pixel data; it persists the Part 10 bytes exactly as received and returns them exactly as stored. Practically observed transfer syntaxes during Phase 1 validation:

Transfer Syntax	UID
Explicit VR Little Endian	1.2.840.10008.1.2.1
Implicit VR Little Endian	1.2.840.10008.1.2
Deflated Explicit VR Little Endian	1.2.840.10008.1.2.1.99
JPEG Baseline (Process 1)	1.2.840.10008.1.2.4.50
JPEG-LS Lossless	1.2.840.10008.1.2.4.80
JPEG 2000 Lossless	1.2.840.10008.1.2.4.90
JPEG 2000	1.2.840.10008.1.2.4.91
RLE Lossless	1.2.840.10008.1.2.5

3.1.3 Request Form

- Method: `POST`
- Path: `/dicomweb/{tenantId}/studies`
- Content-Type: `multipart/related; type="application/dicom"; boundary=...`
- Per-part Content-Type: `application/dicom`

- Authentication: Cloudflare Access JWT in `Cf-Access-Jwt-Assertion` header, OR mutual TLS client certificate (per-tenant policy).
- Tenant resolution: `{tenantId}` in path matches `tenants.slug` registered via the SCC tenant registry (`/api/admin/tenants/registry`).

3.1.4 Response Form

- `200 OK` with `application/dicom+xml` STOW-RS response document enumerating per-instance outcomes (`ReferencedSOPSequence` for accepted, `FailedSOPSequence` for rejected with reason codes per PS3.18 §10.5).
- `401 Unauthorized` if auth fails.
- `403 Forbidden` if the tenant is suspended.
- `413 Payload Too Large` if a single POST exceeds the configured upload ceiling (default 4 GB per body).

3.1.5 Acceptance Semantics

SCC acks `200 OK` ONLY after the Part 10 bytes are durably committed to the SQLCipher hold queue (sealed under IKeyEscrow per §6 below) and the audit-log row is appended (with hash chain — see §6). A pre-commit failure (disk full, scope-key unavailable) returns `500 Internal Server Error` with no row recorded.

3.2 WADO-RS Origin Server

3.2.1 Supported Retrieve Operations

Operation	Path
Retrieve Study (instances)	<code>GET /dicomweb/{tenantId}/studies/{studyUid}</code>

Series-level (`/series/{seriesUid}`), Instance-level (`/series/{seriesUid}/instances/{instanceUid}`), and Frame-level (`.../frames/{frames}`) retrieves are **not** supported in Phase 1. The on-prem Router consumes whole-study fetches; instance-level retrieval is on the Phase 2 candidate list.

Bulkdata, Metadata, and Rendered retrievals are **not** supported.

3.2.2 Response Form

- Content-Type: `multipart/related; type="application/dicom"; boundary=...`
- One part per instance; each part `Content-Type: application/dicom`.
- HTTP/1.1 chunked transfer encoding used; clients should not buffer the full body in memory.
- `200 OK` on success; `404 Not Found` if study is not in queue (TTL expired, never received, or already DELETE-acked).

3.3 QIDO-RS Origin Server

3.3.1 Supported Query Operations

Operation	Path
Search for Studies	<code>GET /dicomweb/{tenantId}/studies?...</code>

Series and Instance searches are **not** supported in Phase 1.

3.3.2 Match Keys

Supported query parameters (PS3.18 §10.6.1.2): - `StudyInstanceUID` (0020,000D) - `StudyDate` (0008,0020) — range queries `YYYYMMDD-YYYYMMDD` - `AccessionNumber` (0008,0050) - `PatientID` (0010,0020) - `limit`, `offset` — pagination

Match semantics are “Single Value Match” and “Range Match” per PS3.4 §C.2.2.2.1. Wildcard matching is **not** supported.

3.3.3 Response Form

- `200 OK` with `application/dicom+json` body containing one JSON object per matched study with the minimum attributes per PS3.18 §10.6.1.3 (Required Matching) plus `00081190` (RetrieveURL) pointing back at the WADO-RS endpoint of §3.2.

3.4 DELETE Channel (Router acknowledgment)

Operation	Path
Drop study from queue	<code>DELETE /dicomweb/{tenantId}/studies/{studyUid}</code>

Not a DICOMweb standard operation — SCC-specific. The Router invokes this once it has successfully forwarded the study to all configured destinations on-prem. Returns `204 No Content` on success; `404` if the study isn't in the queue.

4. Communication Profiles

4.1 Supported Communication Stacks

HTTPS (HTTP/1.1, HTTP/2 negotiated when the client supports it) on TCP/IP. IPv4 and IPv6 both supported. Per-tenant endpoints are exposed via Cloudflare Tunnel; TLS terminates at the Cloudflare edge.

WebSocket (`/relay/{tenantId}`) is the out-of-band notification channel between SCC and the on-prem Router. It is **not** a DICOM channel; the WS frames carry SCC-private JSON envelopes describing studies available in the hold queue.

4.2 TLS

- TLS 1.2 minimum (TLS 1.3 preferred), enforced by Cloudflare edge configuration.
- Cloudflare Access JWT is the default authentication for the admin console + DICOMweb endpoints. Per-tenant mTLS (X.509 client cert issued by SCC's internal CA) is **also** supported and is the recommended posture for production AI-vendor onboarding.
- The internal CA's CSR-sign + keypair-issuance endpoints live under `/api/pki/*` (admin authentication required).

4.3 Physical Media

Internet. No private-link / on-prem direct-connect requirement in Phase 1.

5. Extensions, Specializations, Privatizations

5.1 SCC-Specific Behaviors (beyond PS3.18)

1. **Per-tenant URL prefix** — `/dicomweb/{tenantId}/...` is a Synthology convention to multiplex many AI vendors onto a single SCC deployment. The tenant slug appears in the path; vendors do NOT see other tenants' studies.
2. **WebSocket notification channel** — `/relay/{tenantId}` is proprietary. The on-prem Router is the only intended consumer.
3. **DELETE-as-ack** — see §3.4.

5.2 No DICOM Extensions

SCC does not negotiate extended attributes, does not implement any PS3.18 Annex E (DICOMweb Capabilities) document beyond the routine HTTP `OPTIONS` reply.

6. Configuration

6.1 Tenant Provisioning

A tenant must exist in SCC's tenant registry (`tenants.db`) before its STOW/WADO/QIDO/DELETE endpoints accept requests. Provisioning is done via the operator console (`/tenants`) or `POST /api/admin/tenants/registry` . Each tenant carries:

- `slug` — URL-path identifier (1–128 chars, `[a-z0-9._-]`)
- `display_name` — human-readable
- `contact_email` — privacy / incident contact
- `is_suspended` — when true, all DICOMweb endpoints return 403

6.2 Authentication

Per-tenant configurable. Phase 1 supports: - Cloudflare Access JWT (default; integrates with the customer's IdP via the standard Synthology Cloudflare Access app catalog). - mTLS at the relay handshake (`RelayOptions.RequireClientCert=true`). CA, certificate issuance, revocation ledger all live within SCC.

6.3 Retention + Cold Storage

- `HoldQueueOptions.RetentionHours` — default 72.
- `HoldQueueOptions.ColdStorageDir` — empty by default (delete-only). When set, sweep archives each study as a directory of Part 10 files plus a `manifest.json` before purge.

7. Support of Character Sets

SCC preserves (0008,0005) `Specific Character Set` as received; it does not recode PHI. All ISO-IR-* sets and multi-byte encodings (ISO 2022 series, GB18030) pass through intact. JSON responses (QIDO-RS) are UTF-8 per

8. Security

8.1 At Rest

- Per-tenant SQLCipher databases sealed under IKeyEscrow scope `SynthCloudConnectHoldQueue_<tenant>` (DOC-2026-306 / SPEC-2026-005).
- Internal CA private key sealed under `SynthCloudConnectPki` scope.
- Operator data (audit log, tenant registry, RBAC) sealed under `SynthCloudConnectDataProtection` scope.

8.2 In Transit

- All inbound traffic terminates TLS at Cloudflare edge (per §4.2).
- Internal gateway-to-Router WebSocket can be mTLS at SCC's discretion (config flag `RelayOptions.RequireClientCert`).

8.3 Audit Log

SCC writes a SHA-256 hash-chained row to `audit.db` for every state- changing admin action (tenant create/update/suspend, study delete, PKI sign/revoke, RBAC role/assignment change). Per-row:

```
entry_hash = SHA-256(utc | actor | action | tenant_id | target_id |  
                    outcome_json | prev_hash)
```

Verification endpoint: `POST /api/admin/audit-log/verify` walks the chain and reports `broken_at_id + reason` on mismatch. STOW/WADO/ QIDO/DELETE traffic is **not** logged per-instance to the audit log (volume); per-instance metadata lives in the SQLCipher hold queue.

8.4 Access Control

- 12-permission catalog (`view_tenants` / `manage_tenants` / `view_hold_queue` / `delete_hold_queue` / `view_relay` / `view_pki` / `manage_pki` / `view_audit` / `manage_demo` / `view_settings` / `manage_settings` / `manage_rbac`).
- Per-route `.RequireAuthorization("<perm>")` enforcement.
- Operator email comes from the validated CF Access JWT; role lookup in `rbac.db` . Grant-all fallback while `user_role_assignments` is empty (so the first operator into a fresh install isn't locked out).

9. Identifiers Emitted by SCC

Item	Value	Scope
Implementation Class UID	1.2.826.0.1.3680043.10.1443.5	New for SCC; arc sibling of Router (.1), VNA (.2), IPE (.3), SR Engine (.4).
Implementation Version Name	SYNTHCLOUDCONNECT_1_0	First DICOMweb-only Synthology product.

SCC is a pass-through DICOMweb origin server; the Implementation Class UID above is included in the SCC-generated audit metadata only. SCC does NOT modify Implementation Class UID fields inside the Part 10 payloads it transits — those are preserved exactly as the origin vendor wrote them.

10. Annexes

10.1 Abstract Syntaxes (abbreviated)

Because SCC accepts all Storage SOP Classes, a full enumeration is omitted. Consult PS3.4 Annex B.4 for the authoritative list.

10.2 Non-Conformances

- No classical DIMSE protocols (C-STORE, C-FIND, C-MOVE, C-GET, C-ECHO). SCC is DICOMweb-only.
- No WADO-RS series / instance / frame retrieval (Phase 1 supports whole-study only).
- No WADO-RS Bulkdata, Metadata, or Rendered retrievals.
- No QIDO-RS series or instance search.
- No UPS-RS (Worklist) or MPPS.
- No DICOMweb Capabilities document (PS3.18 Annex H).
- No Storage Commitment.
- No transcoding; pass-through only.

10.3 Tested Peers

Phase 1 interop validation conducted against: - ImageStream Router v1.1.1.91+ (the canonical on-prem consumer) - [tools/inject_test_study.py](#) (synthetic SR documents — internal QA)

Third-party AI-vendor interop tests are scheduled per the customer onboarding playbook; results are recorded in the customer's deployment file (not in this conformance statement).

Review cycle: 1 year, or on any of: new WADO-RS retrieval level (series/instance/frame), new QIDO-RS query level (series/instance), addition of DICOMweb Capabilities document, addition of transcoding, addition of Storage Commitment, addition of UPS-RS. **Next review due:** 2027-05-16.

Regulatory classification. Non-device software under the FD&C Act §520(o)(1)(D) software exclusion. This statement is published by Synthology Healthcare Solutions Group, LLC as a controlled document; the authoritative version is the

approved record in the Synthology quality-management system.