

DOC-2026-445 v5 — XyDromatics De-Identification Engine: DICOM Conformance Statement

Document number: DOC-2026-445 **Title:** XyDromatics De-Identification Engine: DICOM Conformance Statement **Version:** v5 **Category:** DICOM Conformance Statement **Product:** XyDromatics De-Identification Engine **Release version:** 1.0.1.63 **Classification:** Non-device software (FD&C Act §520(o)(1)(D)) **Owner:** Synthology Healthcare Solutions Group, LLC (SHSG) **Effective date:** (on approval) **Review cycle:** 1 year **Next review due:** 2027-07-26 **Supersedes:** v4 (2026-08-01) — first-customer GA version-stamp refresh (RI-2026-433 / DCR-2026-2149); v5 (2026-08-07) — release-alignment to XyDromatics De-Identification Engine 1.0.1.63 (RI-2026-489), canonical DOC-2026-467 masthead, no substantive content change.

This statement is structured per DICOM PS3.2 (Conformance) 2024c; the DICOMweb (STOW-RS) section is structured per PS3.18.

Regulatory posture. XyDromatics De-Identification Engine is **software only — a non-device under FD&C Act §520(o)(1)(D)**. It is not a medical device and has no clinical lane. It transfers and converts medical device data (it de-identifies DICOM objects) but performs no clinical function and produces no diagnostic output. Licensee is responsible for validating the product within Licensee's Quality Management System for Licensee's intended use, including Licensee's own determination under HIPAA §164.514(b).

1. Introduction

1.1 Revision History

Version	Date	Change
1	2026-07-26	Initial release (XyDromatics De-Identification Engine v1.0.x). Documents the Storage SCP (C-STORE receiver) + C-ECHO SCP/SCU, the DICOMweb STOW-RS Origin-Server ingress (RI-2026-353 DCR-A), the egress Storage SCU that forwards de-identified objects to a single downstream destination, DICOM-TLS / mutual-TLS on both legs (RI-2026-353 DCR-B), and the on-egress HIPAA Safe-Harbor de-identification transform.
4	2026-08-01	First-customer GA version-stamp refresh (RI-2026-433 / DCR-2026-2149). Product version updated to 1.0.1.55. No DICOM behavior change: SOP classes, transfer syntaxes, association-negotiation policy, DICOMweb surface, security profiles, and the de-identification transform are identical to 1.0.0.55. UID roots and DICOM version references unchanged.

1.2 Audience

Engineers integrating the XyDromatics De-Identification Engine with DICOM peers — modalities, PACS, routers (e.g. XyDromatics Router), and downstream research archives (e.g. XyDromatics Research VNA). Assumes DICOM familiarity at the PS3.1–PS3.8 level and, for the web ingress, PS3.18.

1.3 Remarks

The XyDromatics De-Identification Engine is a **store-and-forward de-identification node**. It receives identifiable DICOM SOP Instances, removes or replaces the PHI-bearing attributes per an operator-configured HIPAA Safe-Harbor policy, and forwards the de-identified object to a single configured downstream destination. **The object forwarded is deliberately NOT byte-identical to the object received** — de-identification is the product’s core function (see §5). Identifiable data never reaches the downstream archive; de-identification happens in transit, and a de-identification failure or an unhandled residual-PHI risk refuses to forward (fail-closed).

The product is **not** a long-term archive and is **not** a Query/Retrieve provider; it retains no queryable study store. For archival and Q/R semantics see XyDromatics VNA (DOC-2026-075).

Out of scope for this statement. The product also ingests HL7 v2 ORU^R01 reports over MLLP (optionally TLS-wrapped) and applies the same Safe-Harbor free-text and date-shift transforms before forwarding them to

an HL7 sink. HL7 v2 is not a DICOM service and is documented in the product's End User Guide and HW/SW Requirements, not here.

1.4 Terms and Definitions

Per PS3.3. Additional product-specific terms: - **De-identification** — the one-way (non-reversible) removal/replacement of PHI-bearing DICOM attributes per a Safe-Harbor policy (§5). - **Content gate** — a fail-closed classifier that decides, per residual embedded-PHI risk category (encapsulated document, SR narrative, burned-in pixels), whether an object may be forwarded, must be cleaned first, or must be quarantined (§5.5). - **Downstream destination** — the single C-STORE SCU target to which de-identified objects are forwarded (default: XyDromatics Research VNA).

1.5 Conformance References

- DICOM PS3.1–PS3.18, 2024c (esp. PS3.4, PS3.7, PS3.8, PS3.15 Annex E, PS3.18).
- HIPAA Privacy Rule §164.514(b)(2) (Safe Harbor); §164.514(b)(1) (Expert Determination, customer-supplied).
- IHE ITI ATNA (audit) — the product emits ATNA-style audit records for C-STORE receipt and source-node rejection.

2. Implementation Model

2.1 Application Data Flow

The product presents two ingress surfaces and one egress surface. All three share a single de-identification pipeline (`DeidReceiver`):

1. **Classic DIMSE ingress.** An upstream Storage SCU (e.g. XyDromatics Router or a modality) opens a C-STORE association to the De-Identification Engine's Storage SCP (default AE title `DEID_ENGINE` , default port 11128/tcp). Each C-STORE-RQ delivers one SOP Instance bearing real PHI.
2. **Web ingress.** Alternatively, a cross-network sender POSTs a STOW-RS `multipart/related` body to `POST /dicom-web/studies` (default web port 5122/tcp), authenticated by mutual-TLS client-certificate pin and/or a bearer ingest token (§4.2). Each multipart part is one Part 10 object.
3. **De-identification.** For each received instance, the engine applies the Safe-Harbor tag policy in place, recursing into every nested sequence, then stamps PS3.15 §E de-identification evidence (§5).
4. **Content gate.** The de-identified object is classified for residual embedded-PHI risk. Per operator policy the object is quarantined (default), cleaned, forwarded, or rejected (§5.5).
5. **Store-then-drain egress.** The de-identified object is sealed into a durable outbound spool and the inbound C-STORE (or STOW-RS part) is acknowledged Success immediately. A background drain forwards the object to the single configured downstream destination via the egress Storage SCU, with restart-surviving retry/back-off; retry-exhausted objects move to a dead-letter queue for operator re-send.

Because the object is de-identified before egress, its patient identifiers, dates, and — deliberately — its Study/Series/SOP Instance UIDs differ from those received (§5.2). A subject's instances still reassemble downstream because UID remapping is deterministic.

2.2 Functional Definitions

- **Storage SCP** — receives C-STORE associations, hands each instance to the de-identification pipeline; acknowledges Success only after the de-identified object is durably spooled (or quarantined).
- **Verification SCP / SCU** — C-ECHO in both directions (inbound on the SCP port; outbound as a downstream reachability probe).
- **STOW-RS Origin-Server** — accepts DICOMweb store requests at `POST /dicom-web/studies`; each part runs the identical de-identification pipeline.
- **Storage SCU (egress forwarder)** — forwards each de-identified object to the single configured downstream destination.

2.3 Sequencing of Real-World Activities

1. Upstream AE opens an association on the SCP port (default 11128/tcp).
2. The SCP evaluates the source-AE gate. If a Calling-AE allow-list is active (`ScpRestrictUnknownSources` = true AND a non-empty `ScpCallingAeWhitelist`), an unrecognized Calling-AE is rejected with `CallingAENotRecognized`; otherwise the listener is open-receive.
3. The SCP negotiates presentation contexts per §3.1.2.5.
4. Each C-STORE request is de-identified, gated, and — on success — spooled to `<dataDir>/outbound/` (sealed) and acknowledged Success (0x0000).
5. The outbound spool drain subsystem (asynchronous to the SCP) opens a new association to the downstream destination as an SCU and forwards the de-identified object.

3. AE Specifications

3.1 Storage SCP AE

The Storage SCP is provided by the shared `Synthology.Vna.Dicom.Scp` C-STORE listener with the De-Identification Engine's receiver plugged in. It is a receive-only DIMSE service (no Q/R, no Storage Commitment, no MPPS).

3.1.1 SOP Classes Supported

The SCP accepts **all Storage SOP Classes** (PS3.4 Annex B — every Abstract Syntax whose UID begins `1.2.840.10008.5.1.4.1.1.`). There is no built-in Abstract-Syntax allow-list; any Storage SOP Class offered by the association initiator is accepted at negotiation provided at least one common transfer syntax exists (§3.1.2.5.2). This spans, without being limited to, CT, MR, CR/DX, US, NM/PET, XA/XRF, RT objects, Secondary Capture, Encapsulated PDF/CDA/STL, Structured Reporting (Basic Text, Enhanced, Comprehensive, and CAD variants), Key Object Selection, Presentation States, Whole-Slide Microscopy, Segmentation, and Parametric Map.

Additionally supported as SCP:

SOP Class	UID
Verification	1.2.840.10008.1.1

Because the product's function is de-identification, certain SOP Classes carry a high risk of embedded PHI that tag-level de-identification cannot reach (an encapsulated PDF's document stream, a Structured Report's free-text narrative, or burned-in pixel annotations). These are **accepted at the association layer** but are then handled by the fail-closed content gate (§5.5): by default such objects are **quarantined** rather than forwarded. The content gate operates on object content, not on an Abstract-Syntax allow-list — see §3.1.2.7 and §5.5.

Query/Retrieve Abstract Syntaxes (Study/Patient Root FIND/MOVE/GET) are **rejected** at negotiation (`RejectAbstractSyntaxNotSupported`) — the product is not a Q/R provider.

3.1.2 Association Policies

3.1.2.1 General

Parameter	Value
Maximum PDU length (intent)	262,144 bytes (256 KB), config <code>ScpMaxPduLength</code> ; negotiation clamps down to the peer's advertised maximum
Maximum simultaneous associations	10 (config <code>ScpMaxAssociations</code> ; 0 = unlimited, lab only)
Application Context Name	1.2.840.10008.3.1.1.1

3.1.2.2 Number of Associations

- Inbound, simultaneous: 10 max by default (`ScpMaxAssociations` ; hardware-bound; 0 opts back into unlimited).
- Outbound (egress forwarder): one association per drain send to the single downstream destination (§3.2).

3.1.2.3 Asynchronous Nature

The SCP advertises asynchronous operations on the association-accept PDU: `MaxAsyncOpsInvoked = 0` and `MaxAsyncOpsPerformed = 0` (0 = unlimited), so a sending SCU MAY pipeline multiple C-STORE requests on one association. The per-listener `ScpMaxAssociations` cap remains the concurrency bound.

3.1.2.4 Implementation Identifying Information

The product does not override the DICOM Implementation Class UID or Implementation Version Name; the values advertised on associations are those of the embedded fo-dicom 5.2.5 toolkit. Integrators that key on Implementation Class UID (0002,0012) / Implementation Version Name (0002,0013) SHOULD capture the value advertised by their specific deployed build from an A-ASSOCIATE trace rather than rely on a fixed value in this document.

3.1.2.5 Presentation Contexts — Acceptance

3.1.2.5.1 Accepted Abstract Syntaxes

All Storage SOP Classes (PS3.4 Annex B, UID prefix `1.2.840.10008.5.1.4.1.1.`) plus Verification (1.2.840.10008.1.1). Optionally, a per-source SOP-Class allow-list may be configured; when empty (the default) all Storage SOP Classes are accepted. Verification is always accepted regardless of any SOP allow-list.

3.1.2.5.2 Accepted Transfer Syntaxes

Transfer Syntax	UID
Explicit VR Little Endian	1.2.840.10008.1.2.1
Implicit VR Little Endian	1.2.840.10008.1.2
Explicit VR Big Endian (retired)	1.2.840.10008.1.2.2
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 Extended (Process 2 & 4)	1.2.840.10008.1.2.4.51
JPEG Lossless, Non-Hierarchical (Process 14)	1.2.840.10008.1.2.4.57
JPEG Lossless, Non-Hierarchical, First-Order Prediction (Process 14 [SV1])	1.2.840.10008.1.2.4.70
JPEG-LS Lossless	1.2.840.10008.1.2.4.80
JPEG-LS Near-Lossless	1.2.840.10008.1.2.4.81
JPEG 2000 Image Compression (Lossless Only)	1.2.840.10008.1.2.4.90
JPEG 2000 Image Compression	1.2.840.10008.1.2.4.91
RLE Lossless	1.2.840.10008.1.2.5

The product does **not** transcode pixel data. Encoded pixel data is received in, and forwarded out in, whatever transfer syntax was negotiated. Compressed pixel data is **not decoded** on the pass-through path (the pixel codecs are intentionally not registered, keeping the trust surface minimal); see §3.1.2.7 and §9.2 for the one exception (burned-in-pixel cleaning, which requires uncompressed pixel data).

3.1.2.6 Extended Negotiation

Not supported. No SOP-Class Extended Negotiation, no User Identity Negotiation (PS3.7 Annex D.3), no Asynchronous-window sub-item beyond the advertised unlimited values in §3.1.2.3.

3.1.2.7 SOP-Specific Conformance

- **Verification** — standard C-ECHO; always responds Success (0x0000).
- **All Storage SOP Classes** — the SCP requires non-empty (0008,0018) SOP Instance UID, (0020,000D) Study Instance UID, and (0020,000E) Series Instance UID on the received dataset; a missing required UID is rejected (`StorageDataSetDoesNotMatchSOPClassError` / processing failure). On acceptance the instance is de-identified (§5). A C-STORE-RSP of Success (0x0000) is returned only after the de-identified object is durably spooled for forward **or** durably quarantined; a de-identification exception, a content-gate `reject`, an unhandled content-gate risk, or a spool/quarantine-store failure returns a failure status (0x0110 processing failure) so the sender may re-send. This is a deliberate fail-closed contract: the SCP never acknowledges Success for an object it could not safely de-identify, spool, or quarantine.
- **Objects with residual embedded-PHI risk** (encapsulated documents, SR free-text narrative, burned-in pixels) — accepted at the association layer, then routed by the content gate (§5.5). The default disposition for each risk category is quarantine, not forward.

3.2 Storage SCU AE (egress forwarder)

3.2.1 SOP Classes Supported

The egress SCU forwards whatever Storage SOP Class was received (after de-identification). It never synthesizes objects it did not receive. The forwarded object retains its original SOP **Class** UID and negotiated transfer syntax; its instance identity (SOP/Study/Series Instance UIDs) is deterministically remapped by the de-identification transform (§5.2).

3.2.2 Association Policies

- **Destination:** a single configured downstream destination (`Downstream`), addressed by Called-AE-Title + host + port. Default: name `XyDromatics Research VNA` , host `127.0.0.1` , port `11112` , Called-AE `RESEARCH_VNA` , Calling-AE `DEID_ENGINE` , association timeout 60 s.
- **Transfer syntax:** the object is forwarded in its received transfer syntax; on-the-fly transcoding is **forbidden** (pixel pass-through invariant), so a destination that cannot accept the object's transfer syntax will fail negotiation for that instance.
- **Delivery model:** store-then-drain. Objects are forwarded from the durable outbound spool by a background drain with restart-surviving retry/back-off (default: 3 attempts, initial delay 2 s, ×2.0 back-off, capped 30 s). On retry exhaustion the object moves to a dead-letter queue for operator-initiated re-send; it is never silently dropped.
- **TLS:** the egress leg supports DICOM-TLS to the downstream (`Downstream.UseTls` , `Downstream.TlsVerify` , optional client cert/key); default off. See §8.1.

3.3 Verification SCP / SCU

- **SCP:** C-ECHO is accepted on the Storage SCP port and answered Success.
- **SCU:** the product issues C-ECHO to the downstream destination as a reachability probe — both on a background schedule (surfaced in `GET /api/downstream` and `GET /api/health`) and on demand via the operator diagnostics endpoint `POST /api/downstream/echo` . On repeated failure the downstream is reported unreachable; spooled objects remain queued (not dropped) until the downstream recovers.

4. DICOMweb Conformance (PS3.18) — STOW-RS Origin-Server

The product exposes a DICOMweb **Store (STOW-RS)** ingress only. It is **not** a QIDO-RS / WADO-RS / WADO-URI / UPS-RS origin-server (it retains no queryable/retrievable store — see §9.2).

Base path (fixed, not operator-configurable): `/dicom-web/` . STOW-RS is available only when `DicomWeb.Enabled` = true (otherwise the endpoint returns HTTP 503).

4.1 STOW-RS (Store over the Web)

Item	Behavior
Endpoint	POST /dicom-web/studies
Request media type	multipart/related; type="application/dicom" (each part is one Part 10 object)
Unsupported media type	HTTP 415
Missing/blank multipart boundary	HTTP 400
Body size cap	DicomWeb.MaxBodyMegabytes (default 2048 MB)
Source AE attribution	optional X-Calling-AE request header; defaults to STOW-RS
Per-part processing	each part is parsed as a Part 10 object, its required UIDs validated, and handed to the identical de-identification → content-gate → spool pipeline used by the C-STORE SCP (§2.1). Parts are independent — a per-part failure does not fail the batch.
Success response	HTTP 200 when at least one part was accepted
Whole-batch failure	HTTP 409 when no part was accepted

Response body deviation (non-conformance, see §9.2): the response body is a proprietary JSON summary ({ ok, accepted, failed, total, accepted_sop_uids, failures[], received_utc }), **not** the PS3.18 Store-Instances Response (application/dicom+xml / application/dicom+json) with ReferencedSOPSequence / FailedSOPSequence. Integrators parse accepted and failures[] (each carrying sop_uid and a PHI-free reason token) from the JSON. Note that the accepted-instance identifiers reflect the de-identified (remapped) UIDs where applicable.

4.2 Authentication (STOW-RS ingress gate)

The /dicom-web/ prefix is guarded by a dedicated, **fail-closed**, either-mutual-TLS-**or**-bearer gate that is the sole authenticator for the prefix (the admin web-session middleware does not apply to it, so machine ingest is never redirected to a login page and is never anonymous):

- **Mutual TLS (primary):** when DicomWeb.RequireClientCert = true (the default), the client certificate is taken from the TLS handshake, or — for a proxy-terminated pass-through such as Cloudflare Access — from a PEM in the configurable header DicomWeb.ClientCertHeader (default Cf-Access-Client-Cert). The request is accepted only if the certificate's SHA-256 thumbprint is in DicomWeb.PinnedClientThumbprints.
- **Bearer (companion):** when DicomWeb.IngestToken is configured, an Authorization: Bearer <token> matching it by constant-time compare is accepted.
- **Neither configured → every caller receives HTTP 401.** A raw-PHI ingress never serves without a credential.

Unlike a general-purpose DICOMweb archive, this ingress deliberately performs **no PHI airlock / rejection of identifiable content** — a de-identification engine must accept PHI in order to de-identify it. All submitted PHI is de-identified before it leaves the node.

5. Extensions, Specializations, Privatizations

The product's defining behavior is that **the forwarded object is a de-identified derivative of the received object**. This section documents that transform so integrators can predict how objects change between ingress and egress. The transform is **one-way and non-reversible**: no re-identification map (`PhiMap`) and no reversible private-group envelope is ever written. The single re-identification vector is a per-customer master seed held in the product's key-escrow store and never emitted with the data.

5.1 Metadata de-identification (HIPAA Safe Harbor §164.514(b)(2))

A canonical category → tag → action policy is applied at **every** dataset level, recursing into all nested sequences (to a depth guard of 16) so that identifiers hidden in Request Attributes, Scheduled Step Attributes, Original/Modified Attributes, or SR Content sequences are also reached. Per-attribute actions:

Action	PS3.15 basis	Effect
Pseudonymize	value replacement	replace with a deterministic keyed HMAC pseudonym (same value + same seed → same pseudonym, no map retained) — patient/staff names, address/institution/station, telephone, MRN/PatientID/issuer/other-IDs, accession/study ID, device serial
RemapUid	value replacement	replace a DICOM UID with a deterministic <code>2.25.<n></code> UID (keyed HMAC) — see §5.2
Remove (X)	remove attribute	delete the attribute — free-text comment/history tags, health-plan/insurance code sequence, UDI sequence, retrieve URL
Empty (Z)	zero length	set to zero length where structural VR requires a placeholder
Keep	retain (§E.3)	leave unchanged — Patient Sex/Size/Weight, Study/Series Description
AgeCap	value replacement	Patient Age > 89 years → <code>090Y</code> (§164.514(b)(2)(iii))
Date shift	value replacement	see §5.3

All 18 Safe-Harbor identifier categories are enumerated and asserted in the policy; categories with no dedicated DICOM tag (fax, e-mail, certificate/license, IP address) are addressed by removing the free-text tags that would carry them and by the free-text scrubber (§5.4). Private (odd-group) elements are removed at every level by default (`RemovePrivateTags` = true), since vendor-private elements may carry PHI the named policy does not inspect; an operator may retain them under their own §164.514(b) determination.

5.2 UID remapping (consequence for downstream integrators)

Retained source UIDs are themselves a re-identification link (Safe-Harbor category 18), so identifying UIDs are deterministically **remapped**, not preserved: Study, Series, and SOP Instance UIDs, Frame of Reference UID,

referenced SOP Instance UIDs, and similar. **SOP Class UID and Transfer Syntax UID are deliberately NOT remapped** (they are structural, not identifying). Consequences for integrators: - Forwarded objects carry **new** Study/Series/SOP Instance UIDs that differ from those received. - Remapping is deterministic and keyed, so all instances of a study — and repeat studies for the same subject — reassemble consistently in the downstream archive without any retained cross-reference table. - Downstream systems must treat the De-Identification Engine's output UIDs as the authoritative identity of the de-identified copy; there is no supported reverse lookup to the source UID from the data.

5.3 Date handling

Dates are shifted by an interval-preserving, per-subject offset derived from the original Patient ID (so a study and its companion HL7 report shift by the same amount, preserving intervals and ordering). Where no per-subject anchor exists, the transform falls back to year-generalization (DA → YYYY0101, DT → YYYY0101000000, TM emptied). For subjects over 89, the birth date/time (including the birth year) is removed. The shift window is operator-configurable (`DateShiftMaxDays`, default 365).

5.4 Free-text / SR narrative scrubbing

Free-text attributes routinely carrying typed identifiers are removed outright by the policy. Where an operator elects to forward SR objects (rather than quarantine them), the SR free-text narrative (0040,A160) is additionally scrubbed by a best-effort pattern-plus-targeted scrubber. Best-effort narrative scrubbing is not a guarantee; quarantine is the safe default for SR objects (§5.5).

5.5 Content gate (fail-closed)

After header de-identification, the object is classified for residual embedded-PHI risk in three categories — **encapsulated document** (e.g. an encapsulated PDF stream), **SR free-text narrative**, and **burned-in pixel** annotation. Each category carries an operator-configured disposition: `quarantine` (default), `clean`, `forward`, or `reject`; an unclassifiable object defaults to quarantine (fail-closed). An object is forwarded only when **every** applicable category is handled. Cleaning, where enabled and available: - Encapsulated PDF → rasterize pages, OCR-redact, rebuild an image-only PDF (dropping the text layer and document metadata); encapsulated `text/plain` → free-text scrub; any other encapsulated MIME type → fail-closed quarantine. - Burned-in pixels → render frames, OCR the pixel text with a locally bundled engine, and obscure the detected word boxes irreversibly. Supported only for **uncompressed** 8-bit MONOCHROME1/MONOCHROME2 or RGB/YBR pixel data; any other pixel encoding (including compressed transfer syntaxes, which are not decoded) → fail-closed quarantine.

Quarantined objects are stored **sealed and header-de-identified**, so an operator release exposes only the embedded content the operator explicitly accepts — never the header PHI.

5.6 PS3.15 §E de-identification evidence

Every forwarded object is stamped: - (0012,0062) Patient Identity Removed = `YES` - (0012,0063) De-identification Method = `Synthology XyDromatics De-Identification Engine (one-way)` - (0012,0064) De-identification Method Code Sequence = DCM **113100** "Basic Application Confidentiality Profile"; plus DCM **113107** "Retain Longitudinal Temporal Information with Modified Dates Option" **only when** at least one date was genuinely interval-shifted (never merely because a per-subject anchor existed).

5.7 Original Attributes Sequence (0400,0561) — not used for chain-preserve

The product does **not** create an Original Attributes Sequence (or any other provenance/chain-preserve carrier) on the forwarded object. Retaining the original pre-de-identification values would defeat one-way de-identification and reintroduce a re-identification vector. Any Original Attributes Sequence present on an **inbound** object is treated like any other nested sequence and is recursively de-identified (its Modified Attributes Sequence items are scrubbed against the same policy), so PHI cannot survive inside it.

6. Configuration

6.1 AE Title / Ports

Item	Default	Configuration surface
Storage SCP AE Title	DEID_ENGINE	ScpAeTitle (config)
Storage SCP port	11128/tcp	ScpPort (config)
Storage SCP enabled	true	ScpEnabled (config)
Admin/API + STOW-RS web port	5122/tcp	WebPort (config)
DICOMweb base path	/dicom-web/	fixed (not configurable)

Do not confuse `ScpPort` (11128, inbound C-STORE) with `Downstream.Port` (11112, outbound C-STORE SCU).

6.2 Downstream destination

A single destination (`Downstream`) addressed by Called-AE-Title + host + port, with its own Calling-AE, timeout, TLS settings, and forward retry/back-off knobs (`ForwardMaxAttempts` , `ForwardRetryInitialDelaySeconds` , `ForwardRetryBackoffMultiplier` , `ForwardRetryMaxDelaySeconds`).

6.3 Source-AE gate

The SCP is open-receive unless `ScpRestrictUnknownSources` = true **and** a non-empty `ScpCallingAeWhitelist` is configured, in which case only whitelisted Calling-AE titles are accepted. Additional listener hardening knobs: `ScpMaxPduLength` (default 262144), `ScpMaxAssociations` (default 10).

6.4 Observability endpoint (`GET /api/health`)

The product exposes a non-DICOM HTTP observability endpoint, `GET /api/health` (anonymous, PHI-free), for monitoring and capacity planning. Relevant DICOM-adjacent fields include: `scp` (enabled, ae_title, port, bound, error), `dicom_scp` (TLS posture), `downstream` (name, host, port, called_ae, reachable, reachable_ms, reachable_error, checked_utc), `dicom_web` (enabled, base_path, require_client_cert, pinned_count, ingest_token_set), and `queues` (outbound, failed, quarantine, in_flight). This schema is an operator interface, not a DICOM wire protocol, and may evolve across product versions.

7. Support of Character Sets

The product preserves (0008,0005) Specific Character Set as received — it does not recode text. Pseudonyms are ASCII hexadecimal and remapped UIDs are numeric, so replacement values are representable in any DICOM character set. Retained free text in kept attributes (e.g. Study/Series Description) is left in its original encoding. STOW-RS request bodies are parsed as Part 10 objects and inherit the same character-set handling; the JSON response body is UTF-8.

8. Security

8.1 Network

- **DICOM-TLS (secure DIMSE), inbound SCP** — optional (`ScpTlsEnabled` , default off). When enabled, the whole C-STORE association runs inside a TLS 1.2/1.3 channel built from the operator's server certificate; `ScpRequireClientCert` = true upgrades to **mutual TLS**, requiring the peer to present a client certificate whose SHA-256 thumbprint (lowercase hex, no colons) is in `ScpPinnedClientCertThumbprints` (fail-closed: an empty pin set with mutual TLS on rejects every peer). With mutual TLS off, the channel is still encrypted and peer identity is enforced by the Calling-AE gate. When no dedicated SCP certificate path is set, the SCP falls back to the shared in-app web-TLS certificate.
- **DICOM-TLS, outbound SCU** — optional per destination (`Downstream.UseTls` , `Downstream.TlsVerify` , optional client cert/key), default off.
- **STOW-RS ingress** — authenticated by mutual-TLS certificate pin and/or bearer token (§4.2); intended to run over HTTPS (in-app web TLS `WebTlsEnabled` , or a TLS-terminating proxy).

8.2 Audit (IHE ATNA)

The shared SCP writes an audit row per accepted/rejected C-STORE (direction, protocol, remote IP, Calling/Called AE, study UID, accepted/rejected counts, disposition, PHI-free reason). Source-node rejections are audited as security alerts. The product additionally keeps a HIPAA activity log with a 6-year retention floor. Audit records never contain patient identifiers, pre-de-identification UIDs, or free-text reasons.

8.3 Access Control

- **DICOM:** Calling-AE gate (§6.3); optional per-source IP restriction (CIDR) via the shared node model (not populated by default on this product).
- **STOW-RS:** mutual-TLS thumbprint pin and/or bearer ingest token (§4.2), fail-closed.
- **DICOM-level user identity** (PS3.7 Annex D.3 User Identity Negotiation) is not supported; peer identity is established by AE gate and TLS.

9. Annexes

9.1 Abstract Syntaxes

Because the SCP accepts all Storage SOP Classes, a full enumeration is omitted; consult PS3.4 Annex B for the authoritative list. Every Storage SOP Class there is accepted at negotiation provided at least one transfer syntax from §3.1.2.5.2 is offered. Verification (1.2.840.10008.1.1) is accepted in addition. High-embedded-PHI-risk SOP Classes are accepted at negotiation but default to quarantine at the content gate (§5.5).

9.2 Non-Conformances

- No DICOM Query/Retrieve (SCP or SCU) — the product retains no queryable study store.
- No DICOMweb QIDO-RS, WADO-RS, WADO-URI, or UPS-RS — STOW-RS ingress only.
- The STOW-RS response body is a proprietary JSON summary, **not** the PS3.18 `application/dicom+xml` / `application/dicom+json` Store-Instances Response (see §4.1).
- No Storage Commitment (SCP or SCU).
- No Modality Worklist, MPPS, or Unified Procedure Step (UPS).
- No Media Storage / DICOM File-set interchange (PS3.10 physical media).
- No SOP-Class or User-Identity Extended Negotiation.
- Pixel data is forwarded verbatim and is **not** decoded on the pass-through path (compressed transfer syntaxes are accepted and relayed unchanged, not transcoded); burned-in-pixel cleaning is available only for uncompressed 8-bit MONOCHROME1/2 or RGB/YBR pixel data — any other encoding fails closed to quarantine.
- Forwarded objects carry **remapped** Study/Series/SOP Instance UIDs and de-identified metadata; they are intentionally not identical to the received objects (this is the product's function, §5, not a defect — noted here so integrators do not treat the output as an unmodified copy).

Review cycle: 1 year, or on any of: new SOP class handling, DICOM-TLS or STOW-RS authentication changes, addition of a Q/R or DICOMweb query/retrieve surface, Storage Commitment addition, extended-negotiation support, or a change to the de-identification transform semantics (Safe-Harbor policy, UID remap, PS3.15 \$E stamp, or content-gate defaults). **Next review due:** 2027-07-26.

Non-device software under FD&C Act §520(o)(1)(D).

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.