OpenEyes Sensor Product Workflow

OpenEyes Sensor Product Workflow

Field	Value
Distribution	WCT English — OpenC5ISR
Product	OpenC5ISR
Release	0.15.1
Deployment	`openc5isr-en.wallacecorptech.com`
Source	`/srv/wct/releases/OpenC5ISR-v0.15.0`
Evidence	Reference operational demonstration
Source fingerprint	`63d2b1097707e25d666401cdc6362e395968600a40a08690210cd8c0b75fbf50`
Status	Generated baseline — human review required

> **Verification boundary:** This page combines platform design guidance with static evidence from the release. It does not prove that every detected interface is enabled, reachable, secure, or operational in the deployed environment.

Objective

Demonstrate that imagery captured by OpenEyes or uploaded from a phone persists as a sensor product, appears in the OpenEyes product strip, carries source/time/context metadata, and can be associated or pushed to an OpenFiles workspace/release group.

Prerequisites

☐ OpenEyes asset/device session is healthy and authorized.

☐ Local sensor-product storage is writable and persistence survives page refresh/service restart.

☐ Phone upload script has endpoint/token configured outside the script or uses a safe prompt.

☐ OpenFiles target workspace/release group exists and permissions are verified.

Procedure

1. Capture one image from the FPV view and record the asset/session ID and capture time.
2. Verify a thumbnail appears in Sensor Products and opens the full image.
3. Refresh the page and restart only the OpenEyes service; verify the product remains.
4. Run the phone upload script with a uniquely named image and verify it appears in the same product strip.
5. Inspect metadata: product ID, device/uploader, source time, receipt time, MIME type, size, checksum and optional position/track/task.
6. Push the product to the selected OpenFiles workspace/release group and verify recipient access.
7. Verify audit/provenance links from OpenEyes product to the OpenFiles artifact.

Pass criteria

Both captured and uploaded images persist, render correctly, have accurate metadata/checksum, are access-controlled, transfer once without corruption, and retain the source-to-share provenance trail.

Negative tests

- Unauthorized upload or workspace push is rejected and audited.
- Unsupported/oversize/corrupt content is rejected safely.
- Duplicate retry does not create uncontrolled duplicate products.
- Metadata does not expose token, local file-system path or sensitive EXIF beyond policy.

Maintainer Notes

Add human-reviewed deployment notes, corrections, decisions, screenshots, and links here. Content outside the generated block is preserved on future runs.

Revision #1
Created 2026-08-28 15:05:18 UTC by Nexus Ops Administrator
Updated 2026-08-28 15:05:18 UTC by Nexus Ops Administrator