Windows 10 OS upgrade package — SQE sign-off (E2E test plan)

Context

I used this document to drive an end-to-end SQE validation cycle for a Windows 10 in-place upgrade package deployed to Windows-based medication dispensing endpoints (virtual and physical). The goal was to prove upgrade and restore paths were safe across multiple supported application versions and connectivity modes.

Scope

- Validate two deployment modes: cloud-connected (HTTPS) and on-prem queue-based delivery.
- Verify OS and database upgrade steps complete without breaking core workflows.
- Confirm peripheral and security/OS baselines remain stable after the upgrade.
- Capture sign-off expectations across engineering, product, and program roles.

Validation plan (matrix summary)

Connectivity	Coverage	Validated
Cloud-connected (HTTPS)	Representative spread of supported app versions	Preflight checks, upgrade execution, service health, worl
Queue-based delivery	Representative spread of supported app versions	Upgrade + post-upgrade peripherals, lock/drawer behavi
Both	Final-build verification set	Repeatability, “no new defects” signal, release readiness

Acceptance criteria

- Upgrade completes successfully on all representative targets without new Sev 1/2 defects.
- Restore/downgrade path returns the device to a functional baseline.
- Core workflows and peripherals remain operational (scan/print/lock inputs, etc.).
- Key OS/security settings remain in the expected state (where applicable).

Rollback / contingency

- Use the restore mechanism to return the device to its prior baseline if any acceptance criterion fails.
- After restore, re-run a targeted post-restore smoke test (services, workflows, and peripherals) before returning the device to service.

Outcomes / sign-off notes (sanitized)

- Used as a shared definition of “done” for upgrade validation across stakeholders.

- Downstream execution logs and raw sign-off artifacts are intentionally excluded from this portfolio edition.

What this demonstrates

- Release gating via a repeatable validation plan (scope → matrix → execution → sign-off).
- Risk management across multiple deployment paths (cloud vs local delivery).
- Focus on observable outcomes (workflows/peripherals/services) instead of “it installed”.

Redactions performed

- Removed/replaced: names/signatures, internal IPs/hostnames, internal share/URL locations, internal ticket/test-case IDs, and internal tool paths.