Punchout Documentation

PDF Manual

MODULE

punchout

LAST UPDATED

2026-03-29

Authentication and Security Model

Punchout Documentation · /punchout/features/authentication-and-security-model

Punchout uses layered validation so integration errors and unauthorized requests are separated clearly.

Validation Order

1. Resolve buyer profile from inbound identity.
2. Validate protocol identity fields.
3. Validate credentials or shared secret.
4. Validate transport-level constraints (IP, signature, URL policy).
5. Create or resume Punchout context token.

Protocol Identity Check

OCI

- identity is usually bound to buyer id and configured OCI credentials.
- mismatch result: buyer not recognized or credential mismatch.

cXML

- identity is usually mapped from sender credential domain and identity fields.
- mismatch result: sender identity mismatch.

Credential Check

Credentials are configured in typed admin fields and stored encrypted internally.

Expected outcomes:

- valid credential: continue request processing
- missing credential: hard fail with actionable error
- wrong credential: authentication failure

Transport Security Check

Signature validation

- strict mode enforces signed requests.
- recommendation: strict mode enabled in production.

IP allowlist

- only allowed source networks can call inbound endpoints.
- recommendation: use exact platform egress ranges.

Hook URL validation

- return/callback URLs are validated against policy to prevent unsafe redirects.

Practical Production Baseline

- strict signature validation on
- IP allowlist on
- secrets rotated and access-controlled
- trace logging enabled with payload sanitization