Authentication and Security Model

PunchOut Documentation

Guide for Magento administrators, technical project owners, and implementation teams.

LAST UPDATED
2026-08-22

SOURCE
Open this article online

EXTENSION
Magento 2 Extension Punchout

Authentication and Security Model

PunchOut does not accept a request merely because it contains a known buyer ID. Setup requests pass through store resolution, request security, protocol authentication and return-URL validation before a session context is created.

Validation sequence

1. Read the OCI parameters, JSON body or cXML body.
2. Resolve an active buyer by protocol, buyer identity and store scope.
3. Re-check that PunchOut is enabled in the resolved buyer's store.
4. Apply the IP allowlist and optional global HMAC signature.
5. Verify the buyer's OCI or cXML credentials.
6. Apply optional Basic, bearer or shared-secret-header transport authentication.
7. Validate the return URL.
8. Resolve the customer according to the buyer profile and create the expiring context token. E-mail mapping can provision a missing customer when JIT is enabled.

OCI identity

The buyer resolver uses `buyer_id` or `USER`. Authentication then compares the request username with the OCI username on the profile and checks the configured password. OCI protocol fields are independent of an optional HTTP `Authorization` header.

cXML identity

The request extractor reads sender identity, credential domain and shared secret from the cXML header. All three values must match the selected buyer profile. The sender identity also acts as the buyer ID used for profile resolution.

Magento customer identity

The buyer profile selects one customer-resolution mode:

- guest session;
- fixed Magento customer;
- customer e-mail from a configured OCI parameter or cXML field;
- optional request customer ID;
- required request customer ID.

Request customer IDs are accepted only when the corresponding security option is enabled. E-mail mapping first resolves an existing account in the buyer profile's website. If none exists and JIT provisioning is enabled, Magento creates the account in the configured customer group and applies Magento's normal account-confirmation policy.

IP allowlist

The allowlist accepts individual IPv4/IPv6 addresses and CIDR ranges. When the field is empty, every valid source IP is allowed. If Magento runs behind a proxy, verify the resolved client address before enforcing the list; otherwise a correct buyer may be rejected or the proxy address may be trusted too broadly.

Global request signature

Strict signature mode expects an HMAC-SHA256 digest in `X-Punchout-Signature` or `signature`. It is an additional SoftwareSilo check and must be implemented by the calling integration. Missing configuration, a malformed digest and a mismatched digest produce different nested security codes.

Return URL policy

The OCI hook URL or cXML `BrowserFormPost/URL` must:

- be an absolute HTTPS URL;
- contain a resolvable host;
- resolve only to public addresses in production;
- avoid `localhost` and private/reserved IP ranges outside sandbox mode.

Sandbox mode permits local or private targets for controlled testing, but it does not permit plain HTTP. The optional insecure-TLS setting affects certificate verification for outbound document delivery; it does not turn an HTTP URL into a valid one. Confirmation, ASN and invoice delivery use their own configured endpoints, not the browser return URL.

Context token

Successful setup creates a random 64-character token with the configured lifetime. The token binds buyer, store, customer, mapping, protocol, operation and cart context. Treat it as a credential: pass it only over HTTPS, never place it in documentation or tickets, and expire it through `/punchout/session/logout` when the flow is abandoned.

The token is intentionally short-lived and may be cleaned up after expiry. An accepted OrderRequest retains only the encrypted routing and identity data needed for later confirmation, shipment and invoice documents. Fulfilment does not require the original browser session.

Trace payloads are sanitized before storage, but access to Punchout Trace should still be restricted through the dedicated ACL permission.