Security and Idempotency

Punchout Documentation

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

LAST UPDATED
2026-09-26

SOURCE
Open this article online

EXTENSION
Magento 2 Extension Punchout

Security and Idempotency

Use buyer authentication, network restrictions and request signing to decide who may call PunchOut. Use idempotency to make a permitted retry safe. They solve different problems and should not be treated as substitutes.

Security layers

- buyer identity and protocol credentials select and authenticate the procurement account;
- optional Basic, bearer or shared-secret-header authentication protects the HTTP transport;
- the IP allowlist limits inbound network sources;
- optional HMAC-SHA256 signatures detect a missing or altered signed request;
- return-URL validation blocks non-HTTPS and production-local targets;
- context tokens bind browser activation, cart access and cart transfer to one accepted setup;
- Magento pricing remains authoritative unless inbound prices are explicitly enabled.

See Authentication and Security Model for the exact order and request fields.

Request replay keys

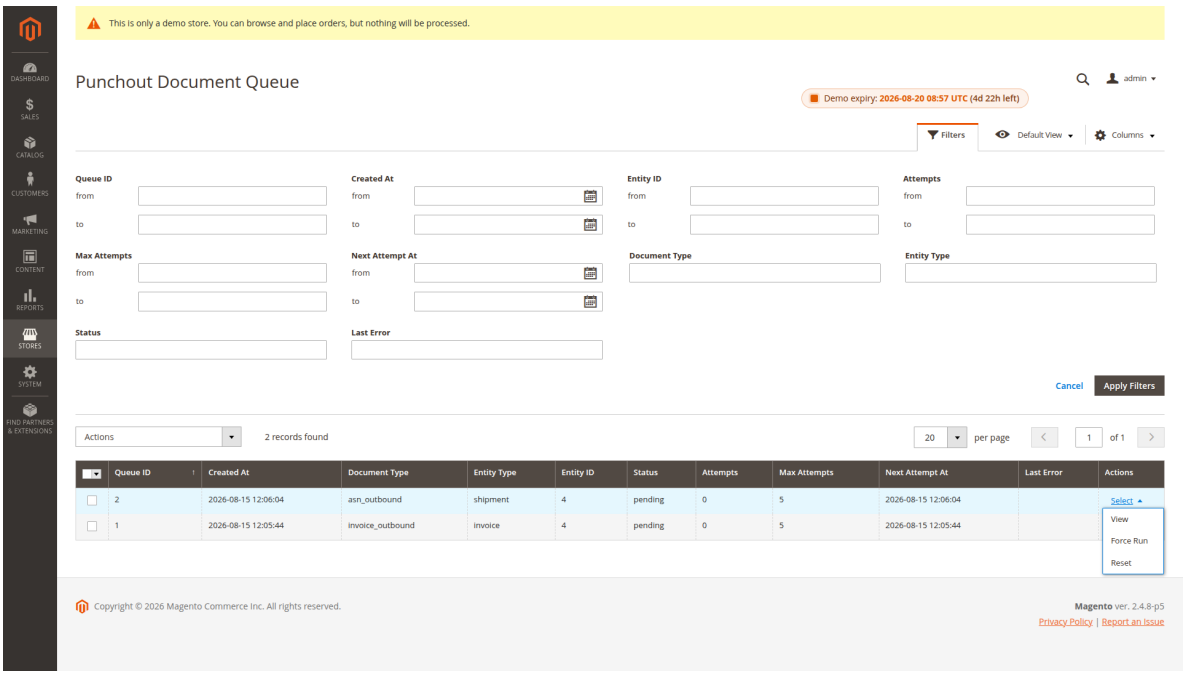
Transfer and document endpoints accept a client-generated key only in the `X-Punchout-Request-Key` header.

The first request reserves the key for that operation. Later calls behave as follows:

- same operation, key and request hash after completion: the saved response and its original HTTP status are replayed;
- same operation and key with a different request hash: HTTP 409 with `PUNCHOUT_REQUEST_REPLAY_CONFLICT`;
- same operation and key while the first call is still running: HTTP 409 with `PUNCHOUT_REQUEST_REPLAY_IN_PROGRESS`.

Generate one key for one semantic action. Reuse it only when retrying the identical request. A buyer must not recycle a key for a changed cart, another shipment or another invoice.

Replay records are isolated by Store view, operation and request key. They are retained according to **Punchout > Configuration > Retention > Request Replay Retention** and removed in bounded batches by the cleanup cron.



Later shipment and invoice documents do not depend on the browser token remaining active. Their encrypted payload and routing information are retained with the order workflow so fulfilment can happen days or weeks after the shopping session.