



Iframe Compatibility Add-On

Punchout Documentation

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

LAST UPDATED
2026-10-13

SOURCE
[Open this article online](#)

EXTENSION
[Magento 2 Extension Punchout](#)

Iframe Compatibility Add-On

Some procurement platforms open the supplier shop inside an iframe instead of a separate browser tab. Browsers and Magento normally restrict this because an embedded shop needs cross-site framing and cookies. The Iframe Compatibility add-on applies the required response and cookie settings only to an authenticated PunchOut context from an explicitly allowed procurement origin.

Normal PunchOut sessions that open Magento as a top-level page do not need this package.

- Composer package: `mageb2b/punchout-iframe`
- Magento module: `MageB2B_PunchoutIframe`
- Required base module: `MageB2B_Punchout`

Install the package

```
composer config bearer.repo.softwaresilo.io <token>
composer config repositories.softwaresilo composer
https://repo.softwaresilo.io/
composer require mageb2b/punchout-iframe:*

php bin/magento module:enable MageB2B_PunchoutIframe
php bin/magento setup:upgrade
php bin/magento setup:di:compile
php bin/magento cache:flush
```

Use the deployment commands required by the current Magento mode and storefront locales.

Uninstalling the package removes the `punchout_iframe_buyer_config` table with all buyer-level origin overrides and the `punchout/iframe/` configuration values. See [Installation](#) for the base module's destructive uninstall scope.

Configure the Store View

Open **Punchout > Configuration > Embedded PunchOut** in Magento Admin.

1. Select the Store View used by the PunchOut buyer.
2. Enable **Iframe Compatibility**.
3. Enter one exact HTTPS origin per line under **Allowed Procurement Origins**.
4. Save the configuration and clear the configuration cache.

An origin contains the scheme, host and optional non-standard port, but no path:

```
https://procurement.example.com
```

```
https://purchasing.example.net:8443
```

HTTP origins, wildcard hosts, credentials, query strings and fragments are rejected. `https://procurement.example.com/app` is not an origin and must not be entered. The add-on normalizes host names, removes duplicate entries and omits the standard HTTPS port.

Override settings for one buyer

Open **Punchout > Punchout Buyers**, edit the buyer profile and expand **Embedded PunchOut**.

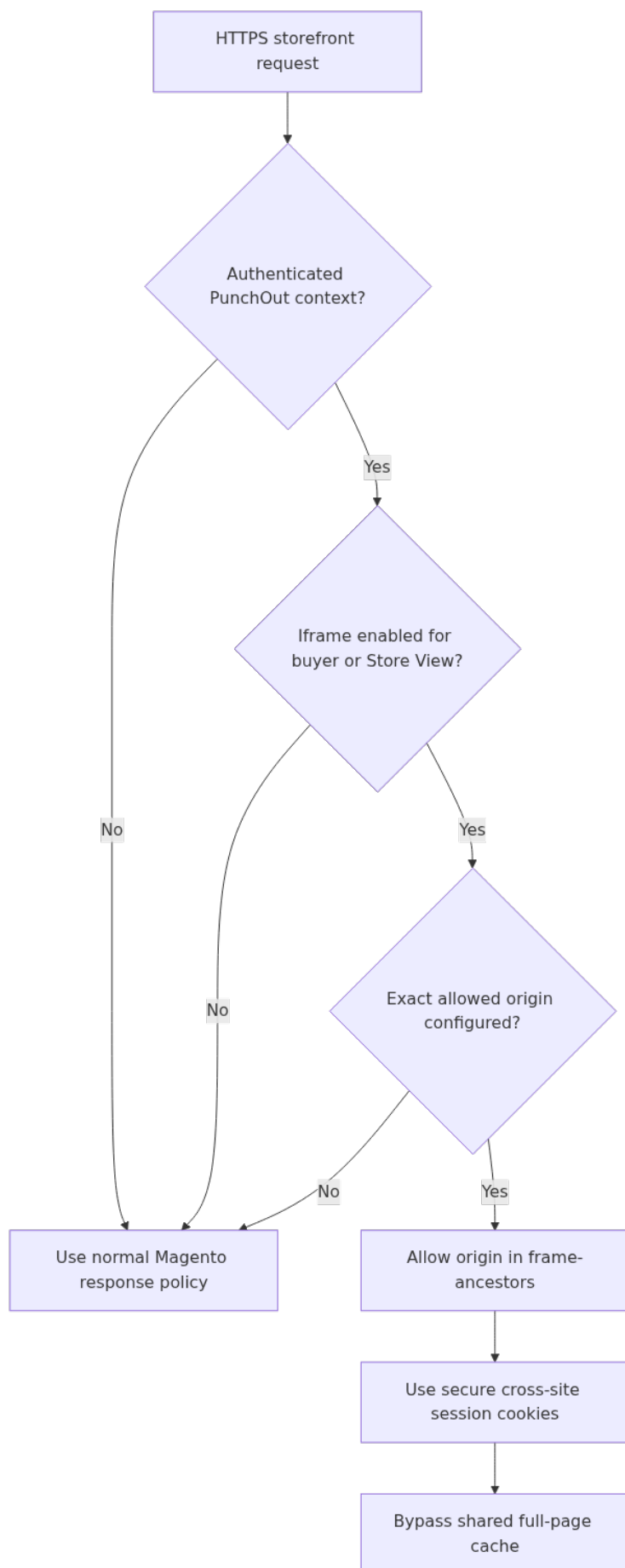
The **Iframe Compatibility** field can inherit the Store View value or explicitly enable or disable embedding for this buyer. **Allowed Procurement Origins** can likewise replace the Store View list for this buyer. Leave the buyer-specific origin field empty to inherit the Store View origins.

Use an override when buyers on the same Store View use different procurement hosts. The buyer profile is the more specific setting and therefore takes precedence over Store View configuration.

Buyer setting	Effective result
Inherit	Use the Store View enablement and origin list
Enabled with origins	Allow only the buyer-specific HTTPS origins
Disabled	Keep this buyer in the normal top-level PunchOut flow

What happens during an embedded session

The add-on does not make every storefront page embeddable. It first confirms that the request uses HTTPS and belongs to a current, authenticated PunchOut context. That context must identify a valid buyer profile and an allowed procurement origin.



For an eligible request, the response allows the configured origin through the Content Security Policy `frame-ancestors` directive. Magento's normal `X-Frame-Options: SAMEORIGIN` header is suppressed for that request. Session and storefront cookies receive the secure cross-site cookie attributes required by modern browsers.

The request also bypasses shared full-page cache. This prevents a response containing one buyer's framing policy from being served to another visitor. Requests outside an eligible PunchOut context retain Magento's normal headers, cookies and cache behavior.

The package does not disable Magento CSP, form keys or customer-session checks.

Configure the procurement platform too

Both applications must permit the embedded relationship:

- Magento must list the procurement application's exact origin.
- The procurement application must allow the Magento storefront in its own iframe or `frame-src` policy.
- The storefront and procurement pages must use HTTPS.
- The browser must accept the cross-site session cookies used by the embedded shop.

Some managed browsers block third-party cookies regardless of the server configuration. If the customer cannot change that policy, configure the procurement system to open the supplier shop in a top-level tab instead.

Session lifecycle

After successful PunchOut activation, the add-on stores a short-lived secure marker for the active context. Its lifetime follows the PunchOut context. A successful cart return removes the marker. Logout and expiry cleanup remove it once the context is no longer usable.

This marker does not authenticate a buyer on its own. The server still validates the underlying PunchOut context for each eligible request.

Troubleshooting

The browser refuses to display Magento in the iframe

Check the response headers in the browser developer tools. Confirm that the request belongs to the active PunchOut session, Iframe Compatibility is enabled at the effective scope, and the parent page's exact HTTPS origin is configured. Also inspect the procurement application's framing policy.

The login or cart is lost inside the iframe

Confirm that every page uses HTTPS and inspect whether the browser accepted the Magento session cookie with secure cross-site attributes. Browser or corporate third-

party-cookie restrictions can still block the session. Test the same PunchOut link in a top-level tab to separate cookie policy from buyer-profile or mapping problems.

The setting works for one buyer but not another

Compare both buyer profiles. An explicit buyer setting overrides the Store View value, including an explicit disabled state or a buyer-specific origin list. Then confirm that each context resolves to the expected buyer profile and Store View.

The regular storefront headers changed

The special response policy must apply only to an eligible embedded PunchOut context. Check whether the request still carries a valid PunchOut token or marker. Clear stale browser data after ending the session, then verify an unrelated storefront request again.

Related guides

- [Authentication and Security](#)
- [Cart API and Session Lifecycle](#)
- [Storefront Operation Policy](#)
- [Common Issues](#)