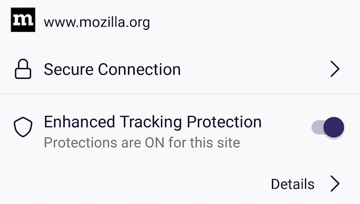
**Firefox Resolution for Keeney’s Punchout Session Returning the Following Error upon Checkout**



Firefox Enhanced Tracking Protection is enabled by default. Enhanced Tracking Protection protects against ad and analytics trackers as well as crypto mining and fingerprinting trackers.

e Procurement solutions require cookies for maintaining session from the eProcurement buyer site and the catalog supplier site. This is creating the false positive where Firefox blocks / removes the previous sites session cookies, usually when returning the cart from your supplier.

The best way to remove the enhanced tracking protection for a e Procurement shopping scenario is to turn off the Enhanced Tracking Protection specifically on eProcurement buyer site and on and the catalog supplier site. Locate the shield on the upper left side of your browser while in logged into the buyer procurement site and turn off Enhanced Tracking Protection and repeat turning off Enhanced Tracking Protection on the catalog supplier site.

By turning off Enhanced Tracking Protection at the site level you do not need to change your security settings or level of protection for any other sites.

1. **Clear your Firefox Browser Cache.**
2. **Close all open Firefox Browser Windows.**
3. **Open a new Firefox Browser window and login into Ariba.**
4. **Take these steps first in your Ariba Session**:

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

1. **Then repeat the process when you reach the punchout landing page:**

**Graphical user interface, application

Description automatically generated**Graphical user interface, application

Description automatically generated